

TECH TOOLS

FOR SMALL FIRMS



BIO

THE POWER OF A SYSTEM

- **JOHN FISHER**

CHECKLIST MANIFESTO

SCAN EVERYTHING

USE A PREDICTABLE NAMING PROCESS

FILES

Name to Maintain Chronological Order

FILE NAMING

Format :

A. Client Initials

B. Date (YYMMDD)

C. Time (if helpful)

D. Nature of File (email, letter, IEP, etc.)

E. Short Descriptor Phrase

F. Number of Pages

LO TS 170304 08 Email Parent to CSE Chair Re IEE 1p.pdf

LO TS 170316 Letter CSE Chair Parent Re Behavior 2p

LO TS 170405 11 Email Teacher to CSE Chair NEEDS BIP! 1p

LO TS 171100 IEE Report 27p

LO TD 171121 14 Audio IEP Meeting



SEARCH EVERYTHING

FREE SOFTWARE

IF YOU CAN'T FIND IT, IT HAS NO VALUE

ADOBE ACROBAT DC

A WORTHWHILE INVESTMENT & TIMESAVING TOOL

BUILD TIMELINES

Annotate Important Information from Each File

ELECTRONIC RETAINER

SAVES TIME AND PROVIDES A STRATEGIC ADVANTAGE



RECORDS

- **INITIAL REQUEST**
- **GOIN WITH LAPTOP AND SCANNER**
- **SCAN & MARK EVERYTHING**

KO FAX

NUANCE POWER PDF ADVANCED

Security

PROTON

SYNC.COM

Efficiency

QUICKPARTS

AND OTHER EXPANDERS





FOCUS

“This is the book I wish I had when I went out on my own in 1995. It would have eliminated a lot of pain.”

—BEN GLASS, ESQ. *Great Legal Marketing*

SYSTEMS

The Power of a

SYSTEM

How to Build the
Injury Law Practice
of Your Dreams

John H. Fisher

THE *NEW YORK TIMES* BESTSELLER

THE CHECKLIST MANIFESTO

HOW TO GET THINGS RIGHT

PICADOR

ATUL GAWANDE

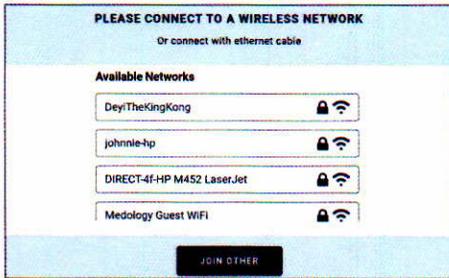
BESTSELLING AUTHOR OF *BETTER* AND *COMPLICATIONS*

Quick Start Guide

Getting started with Raven Scanner

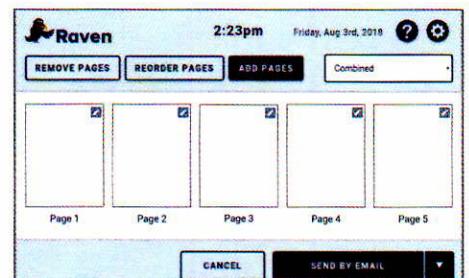
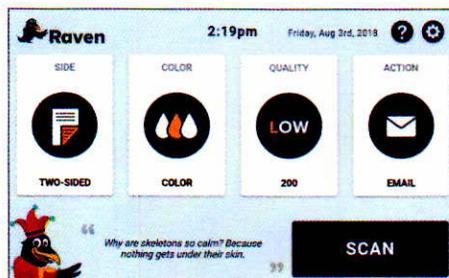
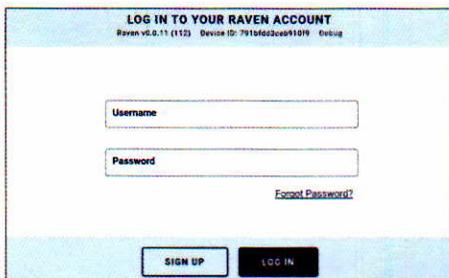


1 Power on and get connected via Ethernet cable or your preferred wireless network.



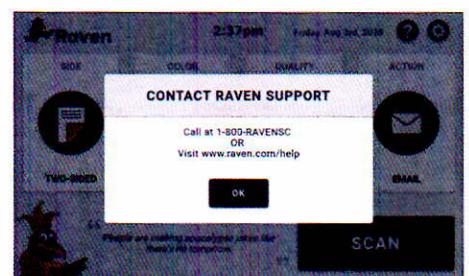
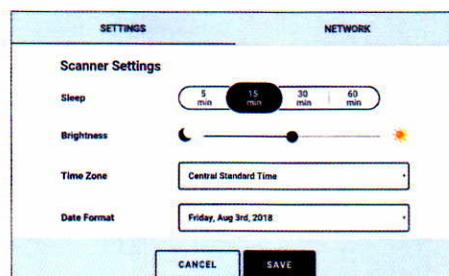
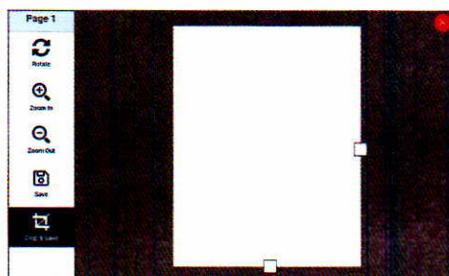
1.1 Connect to available wireless network. 1.2 Connect to other network.

2 Sign in to your Raven account. Sign up if you don't already have an account.



2.1 Sign in to your Raven account or sign up to start a free trial. 2.2 Welcome screen shows scan options, and displays quotes for fun. 2.3 On scan preview screen, you can combine/separate files, rearrange pages, or change file destination.

3 Scan preview shows pages scanned. You can change upload destination options.



3.1 You can edit individual pages by clicking on preview thumbnails. 3.2 Settings allow making changes to the scanner and Network provides options to change current network. 3.3 Help provides 24/7 support via email or live chat.

Version 2



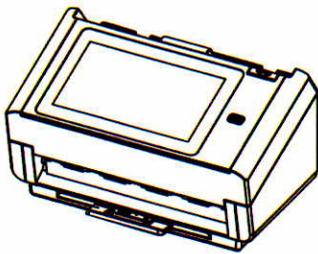
251-1251-0V200

Scanner Setup Guide

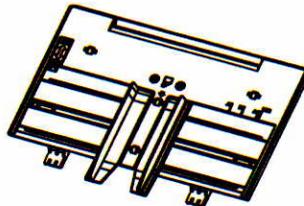
Getting started with Raven Scanner

 **RavenScanner
Pro**

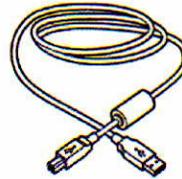
1 What's in the box



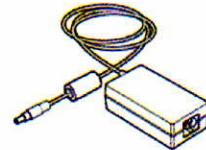
Scanner Main Unit



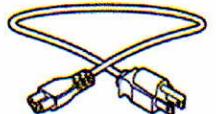
Paper Tray



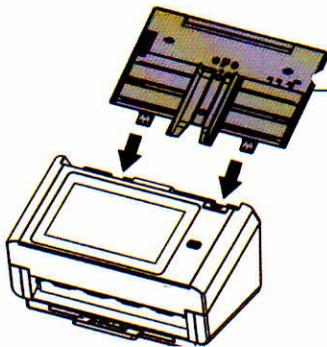
USB Cable



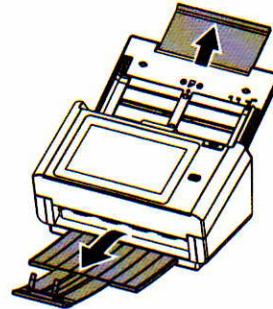
Power Adapter & Power Cable



2 Install the scanner

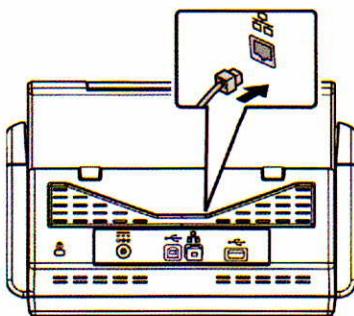


2.1 Hold the ADF Paper Tray and insert two pins to the holes on the top of the scanner as shown.

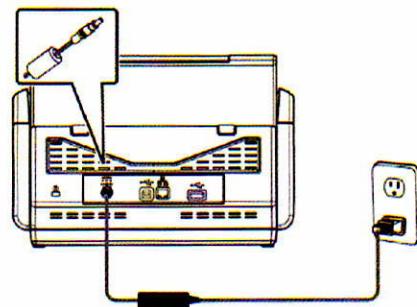


2.2 Pull out the extension to the length of the document. Pull the Output Tray and raise the paper stopper to prevent the paper from falling.

3 Connect to the power



3.1 Connect one end of your Ethernet LAN cable to an available port of your Ethernet Hub, connect the other end to port marked  at the back of the product.



3.2 Connect one end of the power cable to the power receptacle of the product. Connect the other end to an appropriate power outlet.



The Fujitsu fi-7700 Scanner with flatbed



100 ppm/ 200 ipm
in landscape (12"x17" mode)

Fujitsu fi-7700
with 12"x18" flatbed

List Price

\$ 7,995

Your Price

\$ 6,395

BUY NOW

Call or Request a Quote

1-877-4935

Leasing as low as \$154 a month with
no payment until Jan. 2019*

**FREE
SHIPPING**

Includes 90 day
onsite warranty



Everything

- [Installing Everything](#)
- [Using Everything](#)
- [Command Line Interface](#)
- [Command Line Options](#)
- [Customizing](#)
- [ETP](#)
- [Everything Service](#)
- [File Lists](#)
- [Folder Indexing](#)
- [HTTP](#)
- [Indexes](#)
- [INI](#)
- [Keyboard Shortcuts](#)
- [Multiple Instances](#)
- [Options](#)
- [Previous Versions](#)
- [Recent Changes](#)
- [Results](#)
- [Run History](#)
- [SDK](#)
- [Search History](#)
- [Searching](#)
- [Supported Languages](#)
- [Translating](#)
- [Troubleshooting](#)
- [Uninstalling Everything](#)
- [What's New](#)

Everything

The screenshot shows the Everything search engine window titled "parent:c:\windows\system32 *.exe - Everything". The window displays a list of files with columns for Name, Path, Size, and Date Modified. The file "notepad.exe" is highlighted. The status bar at the bottom indicates "Size: 210 KB, Date Modified: 10/07/2015 9:00 PM, Path: C:\Windows\System32".

Name	Path	Size	Date Modified
control.exe	C:\Windows\System32	115 KB	10/07/2015 9:00 PM
winver.exe	C:\Windows\System32	57 KB	10/07/2015 9:00 PM
SlideToShutDown.exe	C:\Windows\System32	20 KB	10/07/2015 9:00 PM
LanguageComponentsInstallerComH...	C:\Windows\System32	43 KB	10/07/2015 9:00 PM
Fondu.exe	C:\Windows\System32	98 KB	10/07/2015 9:00 PM
OpenWith.exe	C:\Windows\System32	83 KB	10/07/2015 9:00 PM
notepad.exe	C:\Windows\System32	210 KB	10/07/2015 9:00 PM
fodhelper.exe	C:\Windows\System32	48 KB	10/07/2015 9:00 PM
lpremove.exe	C:\Windows\System32	67 KB	10/07/2015 9:00 PM
lpksetup.exe	C:\Windows\System32	770 KB	10/07/2015 9:00 PM
DataExchangeHost.exe	C:\Windows\System32	155 KB	10/07/2015 9:00 PM
PrintIsolationHost.exe	C:\Windows\System32	76 KB	10/07/2015 9:00 PM
dialer.exe	C:\Windows\System32	36 KB	10/07/2015 9:00 PM
printui.exe	C:\Windows\System32	63 KB	10/07/2015 9:00 PM
tcmsetup.exe	C:\Windows\System32	16 KB	10/07/2015 9:00 PM
printfilterpipelinesvc.exe	C:\Windows\System32	868 KB	10/07/2015 9:00 PM
spoolsv.exe	C:\Windows\System32	764 KB	10/07/2015 9:00 PM
PrintDialogHost3D.exe	C:\Windows\System32	22 KB	10/07/2015 9:00 PM
TapiUnattend.exe	C:\Windows\System32	14 KB	10/07/2015 9:00 PM
PrintDialogHost.exe	C:\Windows\System32	31 KB	10/07/2015 9:00 PM
ntprint.exe	C:\Windows\System32	62 KB	10/07/2015 9:00 PM
GamePanel.exe	C:\Windows\System32	541 KB	10/07/2015 9:00 PM
SndVol.exe	C:\Windows\System32	240 KB	10/07/2015 9:00 PM

"Everything" is a filename search engine for Windows.

How is Everything different from other search engines

- Small installation file.
- Clean and simple user interface.
- Quick file indexing.
- Quick searching.
- Quick startup.
- Minimal resource usage.
- Small database on disk.
- Real-time updating.

Accelerate Your Productivity with X1 Search

- Advanced Search Commands
- Metadata Column Filtering
- Date Range Filtering
- Saved Searches
- Exporting Results
- Keyboard Shortcuts



X1 Search User Interface

The screenshot displays the X1 Search User Interface within an email client. The top navigation bar includes a search bar with the text "Search Everything - Email" and various action buttons like "New Email", "Open", "Reply", "Reply All", "Forward", "Delete", "Mark Read", "Mark Unread", and "Move". Below the navigation bar, there are tabs for "All", "Email", "Email and Attachments", "Files and Attachments", "Documents", and "Inbox".

The main content area is divided into two sections. On the left is a "Filter Saved Searches" sidebar with a tree view showing categories like "Everything", "Email", "Outlook", and "Files". The "Outlook" category is expanded, showing a list of folders such as "All Email", "Attachments", "Inbox", "Sent Items", "Contacts", "Calendar", "Tasks", "Notes", "MSG Files", "Files", and "Documents".

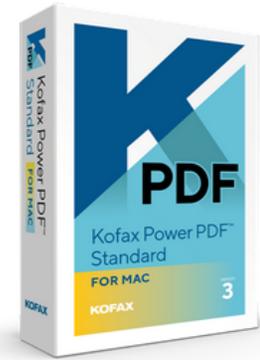
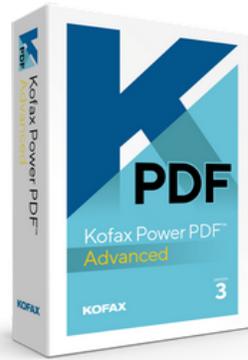
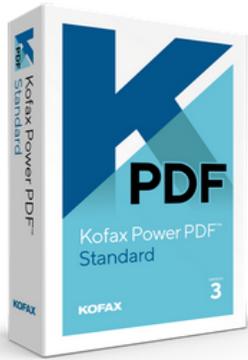
The central part of the interface is a table of search results for "Outlook Email". The table has columns for "Folder...", ".com>", "To", "Subject", "Size", "Attac...", and "Rec...". The results list several emails from "X1 Webinars <in...>" by "Chris Scott <csc...>" with subjects like "Webinar Tomorr...", "Live Webinar | X...", and "Register Today |...".

On the right side, a detailed view of an email is shown. The subject is "Webinar Tomorrow | X1 Search Skills to Accelerate your Business Productivity Webinar". The sender is "X1 Webinars" with the email address "info@x1.com". The email content includes a link to view the email as a web page and a promotional message: "Join us to learn ways to rapidly improve your business Search skills". The main body of the email features the text "Accelerate your Search Skills for Business Productivity" and "Live webinar" with the date and time "Wednesday, January 29 at 10:00am PT / 1:00pm ET - 30 min complimentary event".

At the bottom of the interface, there is a status bar showing "17,297 items indexed", "1 of 26" items displayed, a zoom level of "100%", and a "View" button.



Power PDF Makes Financial Sense
Why pay monthly subscription fees for something you can own now?



Power PDF Standard

For fast and accurate conversion and editing, Power PDF Standard has the most accurate PDF to Word or Excel conversions of any PDF solution. Users can combine, edit, assemble, fill forms and share PDF files, as well as scan paper to PDF and create searchable PDF files.

[Learn More](#)

[Free Trial](#)

\$129

[BUY NOW](#)

Power PDF Advanced

For enhanced security and collaboration, Power PDF Advanced includes all the features of Power PDF Standard, as well as additional features for connectivity, real-time collaboration, security and redaction.

[Learn More](#)

[Free Trial](#)

\$179

[BUY NOW](#)

Power PDF Advanced: Volume Licensing

For enterprise deployment with a single license to manage, Power PDF Advanced: Volume Licensing makes it easy for businesses to create, edit and assemble documents across any platform or device to create workflow continuity both internally and externally.

[Learn More](#)

[Free Trial](#)

[GET A QUOTE](#)

Power PDF Standard for Mac

For fast and accurate conversion and editing specifically designed for Mac with the same powerful features and benefits of Power PDF Standard.

[Learn More](#)

[Free Trial](#)

\$129

[BUY NOW](#)

Find the PDF Solution that's Right for You



Feature	Standard	Standard for MAC	Advanced	Volume Licensing
Easy-to-use, Office-style interface optimized for Windows 10 and touchscreen devices.	✓		✓	✓
Create and compile PDF files from almost any document or file type, including multiple files into a single PDF.	✓	✓	✓	✓
Easily convert PDF files to other formats including Word, Excel, PowerPoint, images and more.	✓	✓	✓	✓
Convert JPG files to PDF or convert PDF to JPG.	✓	✓	✓	✓
Edit and enhance PDF documents to change text, pictures, add annotations, apply stamps and more.	✓	✓	✓	✓
Digital and stamp-based signatures for PDF documents.	✓	✓	✓	✓
Sign and send PDFs for signature using DocuSign®.			✓	✓
Take advantage of cloud connectivity to popular services such as Box, Evernote, Google Drive and Microsoft OneDrive.			✓	✓
Collaboratively create and edit PDFs in real-time with users on the same network.			✓	✓
Connect to popular enterprise document management systems such as SharePoint and NetDocuments.			✓	✓

Redact sensitive information from documents.				
Apply Bates stamping to a single document or a complete set of documents.				
Automate PDF creation jobs using a watched folder.				
Automate PDF workflows, processing and business system connectivity using Kofax AutoStore enterprise capture solution.				
Volume discounts available.				
Supports Citrix, Microsoft App-V and Windows Server network deployment.				
Comes with customization kit for more flexible configuration.				
MSRP	\$129 BUY NOW FREE TRIAL	\$129 BUY NOW FREE TRIAL	\$179 BUY NOW FREE TRIAL	Call for a quote GET QUOTE FREE TRIAL

New XPS 15 7590



4.1 (2619)

[Ask a question](#)

Pushing innovation to the edge.

The world's smallest 15.6-inch performance laptop with a stunning OLED display option. Now featuring 9th Gen Intel® Core™ processors.

Questions about delivery dates? We're here to help. Call 1-866-666-5719 or [Click to Chat](#).

Starting at \$967.99

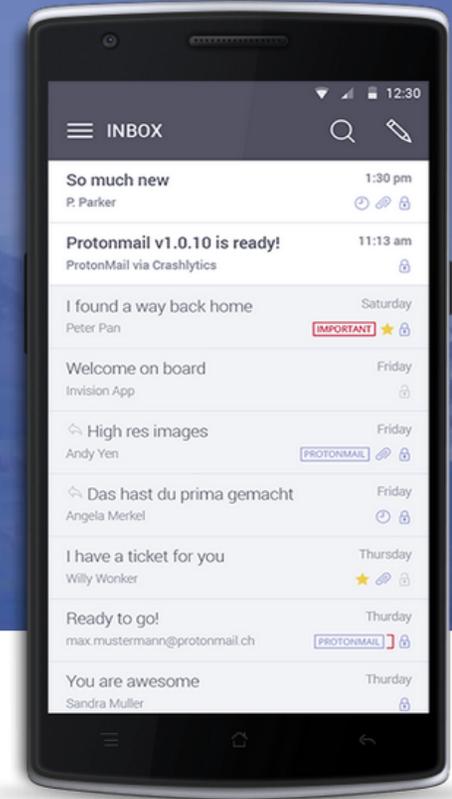
[Get Pre-Qualified](#) | [Apply for credit](#)



Secure Email Based in Switzerland

Secure Your Communications with ProtonMail

GET YOUR ENCRYPTED EMAIL ACCOUNT



The ProtonMail mobile apps are now available worldwide.

Introducing Encrypted Email for Your Mobile Device

Get the Android App

Get the iOS App

Use the Web Version



Swiss Privacy

Data Security and Neutrality



End-to-End Encryption

Automatic Email Security



Anonymous Email

Protect Your Privacy

ProtonMail is incorporated in Switzerland and all our servers are located in Switzerland. This means all user data is protected by strict Swiss privacy laws.



Open Source

Free Secure Email

We believe email privacy should be available to all. That's why our code is open source and basic ProtonMail accounts are always free. You can support the project by [donating](#) or [upgrading to a paid account](#).

All emails are secured automatically with end-to-end encryption. This means even we cannot decrypt and read your emails. As a result, your encrypted emails cannot be shared with third parties.



Easy to Use

Security without the hassle

ProtonMail can be used on any device without software install. ProtonMail secure email accounts are fully compatible with other email providers. You can send and receive emails normally.

No personal information is required to create your secure email account. By default, we do not keep any IP logs which can be linked to your anonymous email account. Your privacy comes first.



Modern Inbox Design

Security with Productivity

The ProtonMail inbox is optimized for productivity. Each detail within our secure email service is optimized to help you better read, organize, and send email.

The ProtonMail Guide to IT Security for Small Businesses

Adopt top IT security solutions for small businesses



Adopt top IT security solutions for small businesses

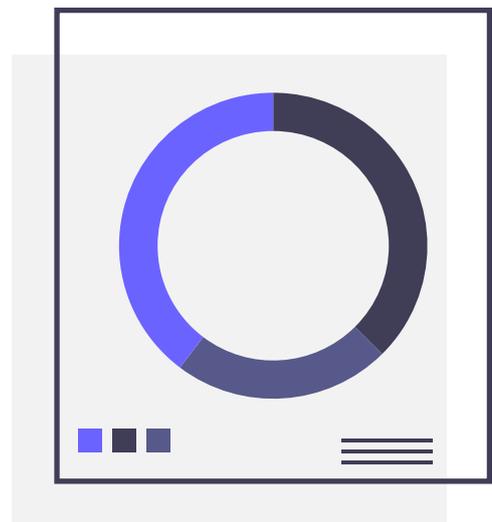
READ THIS CHAPTER to see all the different apps, programs, and services that offer your company increased IT security and data protection. This list includes both free and paid services for

- Communications
- Storage
- Productivity
- Security
- Advanced network security

We made this the last chapter of our ebook because IT security is primarily about creating a [culture of IT security awareness](#). Merely switching to encrypted services will not solve all of your IT security issues. The previous four chapters that describe how to implement IT security best practices form the foundation of a sound IT security policy. However, the following encrypted services will reduce your company's exposure, and, when paired with a security-conscious workforce, can go a long way to preventing a data breach or hack.

Note that while some of these tools will be good solutions for companies of any size, others will work best for smaller businesses that have not

created their own internal network. We describe some tools that [larger companies can use to secure their network](#) (See Chapter 3), but other tools will require expert help to implement correctly.



Communication

Email provider

Most small businesses rely on emails to handle both their internal and external communications. [Email security best practices](#) are essential to keeping your business's data safe, but some email providers can offer your company more security than others.

ProtonMail

[ProtonMail](#) offers its users automatic [end-to-end encryption](#). Your emails are encrypted before they leave your device so that only you and your intended recipient can access them. You can even secure your [messages to non-ProtonMail users](#) by sending password-protected emails.

Platforms:

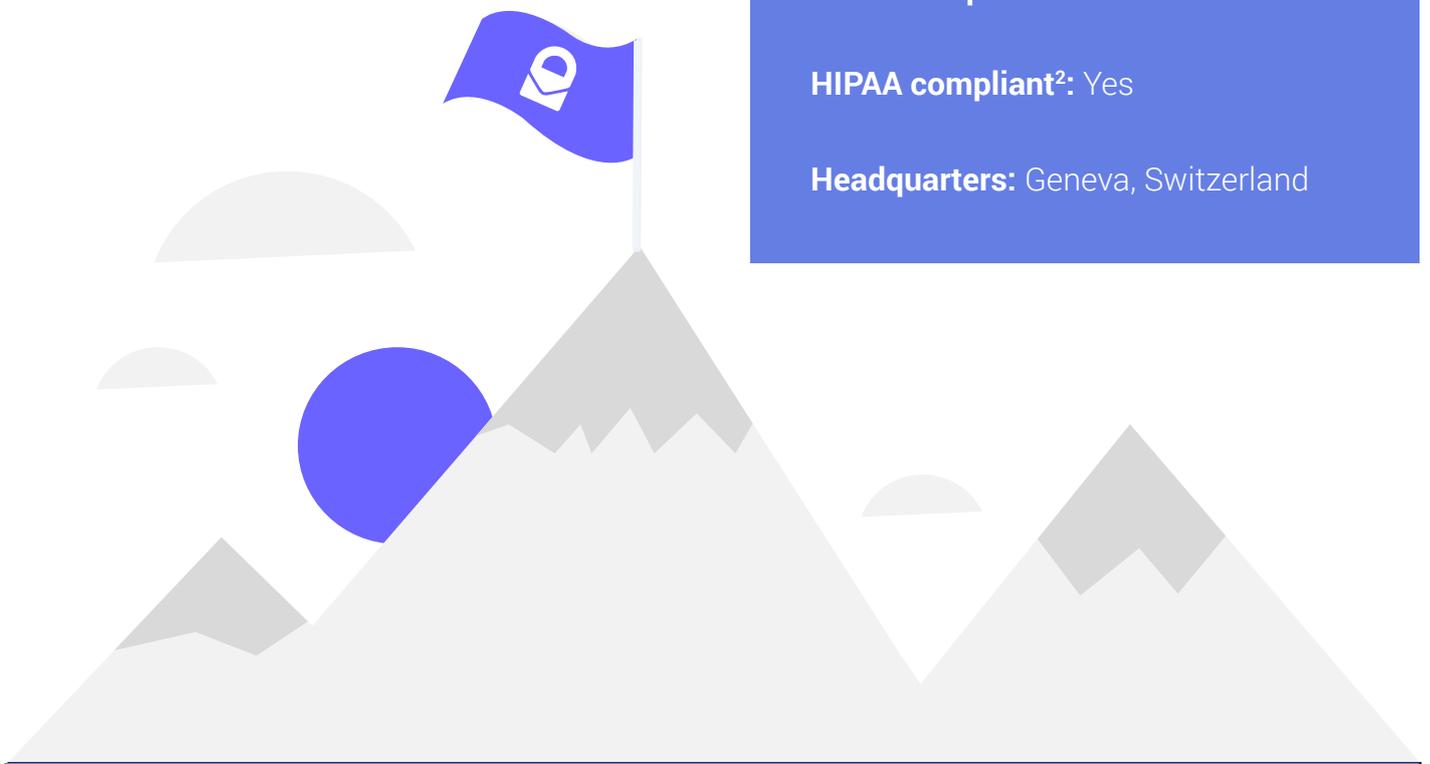
Android, iOS, and web app. Also has [Bridge integration](#) with Microsoft Outlook, Mozilla Thunderbird, and Apple Mail

Price: Has a free option. Premium plans begin at \$5 per user per month.

GDPR compliant¹: Yes

HIPAA compliant²: Yes

Headquarters: Geneva, Switzerland



1 This signifies that this tool adheres to the technical safeguards defined in the GDPR guidelines, which means that it can contribute to an organization complying with GDPR. It does not mean that just by using this tool your organization will be GDPR compliant.

2 This signifies that this tool adheres to the technical safeguards defined in the HIPAA guidelines, which means that it can contribute to an organization complying with HIPAA. It does not mean that just by using this tool your organization will be HIPAA compliant.

Team collaboration

Many businesses have employees and contractors working remotely. This can make coordinating a challenge unless you use a team collaboration app. Given the amount of information that can be exchanged and stored on these platforms, using one that is encrypted is a necessity.

Wire

[Wire](#) is one of the only end-to-end encrypted services that allows for group calls, which makes it more secure than Slack when trying to manage team communication. Wire has been independently audited and is entirely open source, giving you some assurance that Wire's code is doing exactly what they say it is.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at €6 per user per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Zug, Switzerland

Messaging

For companies that do not need all the functionality of a collaboration app but still want their communications to be secure, there are end-to-end encrypted messaging apps.

Signal

[Signal](#) is widely considered to be the most secure encrypted messaging app. It supports texts, group texts, as well as voice and video calls. Conference calls between more than two people, however, are not possible.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Free

GDPR compliant: Yes

HIPAA compliant: Yes (with caveats)

Headquarters: Mountain View, California, USA

Threema

[Threema](#), unlike Signal, does not require a phone number to create an account, which means Threema is as close as you can get to truly anonymous messaging. The company headquarters is in Switzerland, giving its service strong legal privacy protections.

Platforms: Android, iOS, Windows phone, and web app

Price: Starts at 1.40 CHF per device per month

GDPR compliant: Yes

HIPAA compliant: No

Headquarters: Zurich, Switzerland

Storage

Cloud storage

Cloud storage has redefined how offices can work. By storing files on the cloud, your business can maintain a backup of all critical documents in case of a catastrophic system failure as well as easily share documents and sync progress between different employees. Protecting these files and the data they contain should be one of your business's top priorities.

Tresorit

[Tresorit](#) is an end-to-end encrypted cloud storage service. It has optimized its service for businesses, allowing you to create different levels of access for various documents and to revoke users' and devices' access to files.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Starts at \$25 for two users per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Zurich, Switzerland

Sync

[Sync](#) is another end-to-end encrypted cloud storage service, similar to Tresorit. It gives businesses admin control, allowing supervisors to create different levels of access for different employees. Sync also allows you to preview your files before you open them.

Platforms: Android, iOS, macOS, and Windows

Price: Starts at \$10 per user per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Toronto, Canada

Boxcryptor

[Boxcryptor](#) is slightly different. It allows you to encrypt your documents before you save them on a separate cloud service, like DropBox or Google Drive. Your team can still easily collaborate and share files over the cloud, but now your documents are secure.

Platforms:

Android, iOS, Linux, macOS, Windows, and a Chrome web browser add-on

Price: Starts at \$600 for five users per year. (There is also an individual Business plan that is \$96 per user per year, but it has less functionality.)

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Augsburg, Germany

Cryptomator

[Cryptomator](#) is the free, open source version of Boxcryptor. With Cryptomator, your employees can create a virtual hard drive that is connected to a folder (called a "vault") on their cloud storage service and protect it with a password. Any document they drag and drop into the virtual hard drive is automatically encrypted and backed up in the vault. There is also [Cryptomator Server](#), for larger businesses

Platforms: Android, iOS, macOS, and Windows

Price: Free (There is a one-time fee of \$9.49 to download the Android app and \$9.99 to download the iOS app.)

GDPR compliant: Yes

HIPAA compliant: Yes

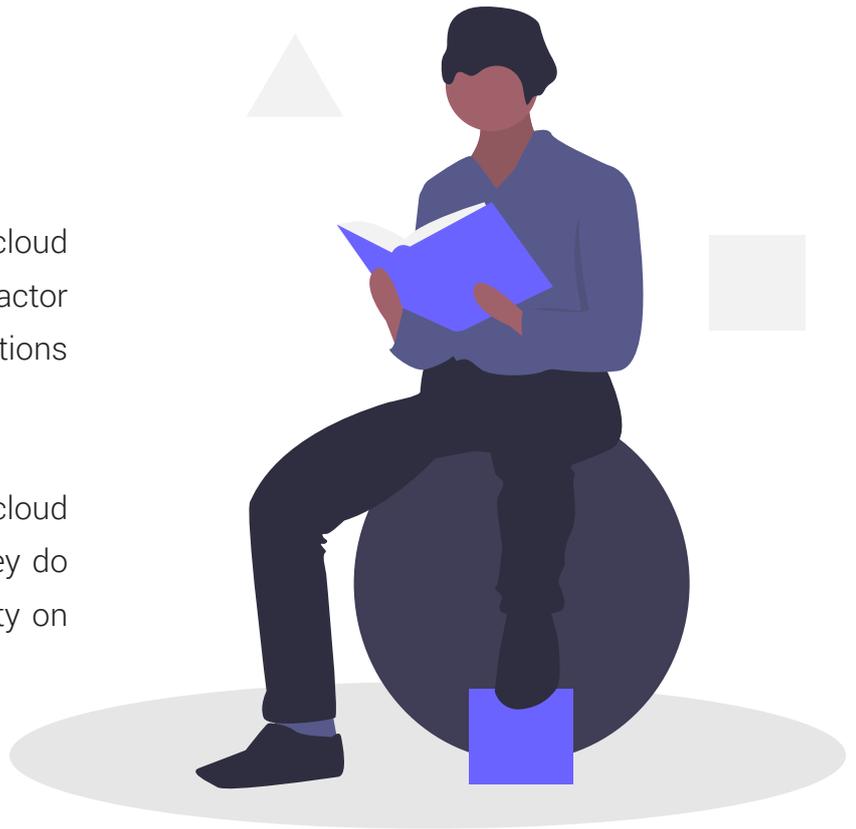
Headquarters: Sankt Augustin, Germany

looking to add encryption to the files on their company servers.

Other cloud services

pCloud is an end-to-end encrypted cloud service. It is GDPR compliant, allows two-factor authentication, and its business subscriptions start at \$7.99 user/month/TB.

Spideroak is an end-to-end encrypted cloud storage service similar to Tresorit, but they do not offer two-factor authentication security on their accounts.



Productivity

Notepad

Also known as a “text editor,” a notepad is a program that allows you to write and edit plain text. A notepad can be used to keep notes, write documents, and alter configuration files or programming language source code.

Standard Notes

[Standard Notes](#) is a simple, end-to-end encrypted note-taking app that can sync your notes across all your devices. Its clean interface and numerous extensions mean that you can use Standard Notes for everything from writing yourself reminders to coding.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Has a free option. Premium plans begin at \$9.99 per user per month.

Headquarters: USA

Joplin

[Joplin](#) is another end-to-end encrypted note-taking app, but unlike Standard Notes, users must manually activate the end-to-end encryption feature. Joplin relies on external services, like NextCloud or Dropbox to synchronize across devices.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Free

GDPR compliant: Yes

Headquarters: N/A

Security

VPN

A virtual private network is an effective way to add a layer of encryption to your online activity. It also allows your employees to safely work on public WiFi while they are on the road.

ProtonVPN

[ProtonVPN](#) secures your Internet connection with AES 256-bit encryption, the industry gold standard, and its use of Perfect Forward Secrecy means that even if your traffic is intercepted and saved, it can never be decrypted at a later date.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Has a free option. Premium plans begin at \$5 per user per month.

Headquarters: Geneva, Switzerland

Password manager

Creating [strong, unique passwords](#) or [passphrases](#) for your accounts is one of the basics of IT security, but no employee can remember all the passwords necessary to log in to all the platforms they need to use for work. (Look how long this list is already!) A password manager changes all that. By safely encrypting all your passwords, a password manager allows you to create passwords that are impossible to crack, without having to remember them all. Using a trustworthy password manager to secure your passwords is one of the easiest ways to improve your company's security.

Bitwarden

[Bitwarden](#) is an open source, end-to-end encrypted password manager. It helps your employees create randomly generated passwords for all of their accounts, and then syncs those passwords across all their devices.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at \$5 for five users per month

Headquarters: Florida, USA

1Password

[1Password](#) is another end-to-end encrypted password manager, but it has a few more bells and whistles. While it is only a paid service, it is considered to be one of the most secure password managers. Its Watchtower feature will alert you if any of your passwords have been exposed in recent data breaches.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at \$3.99 per user per month

Headquarters: Toronto, Canada

Dashlane

[Dashlane](#) is also a premium end-to-end encrypted password manager. It will scan known security breaches and will send you an alert if it finds any of your passwords among those exposed. Its business plan also comes with an admin console that allows you to set permission levels for all your employees.

Platforms: Android, iOS, macOS, Windows, and web browser add-ons

Price: Starts at \$4 per user per month

Headquarters: New York City, USA

Other password managers

LastPass: A premium password manager, but it does not alert its users if their password is exposed in a data breach.

KeePass / KeePassXC: These are both free, open source password managers, but neither of them offers official mobile apps.

Two-factor authentication

To ensure your critical accounts are secure, you should enable two-factor authentication (2FA) in addition to using a strong, unique password. The site [Two Factor Auth](#) will help you identify which services you can use 2FA on. By using 2FA on your accounts, you can prevent intruders from accessing your accounts even if they get a hold of your passwords.

YubiKey

[The YubiKey](#) is a hardware token (a specialized USB stick) that you can plug into your device to confirm your identity. While it is thought to be the most secure form of 2FA, relatively few services support hardware token 2FA.

Platforms: YubiKey 5 NFC works with macOS, Windows, and NFC-equipped Android and iOS devices

Price: A YubiKey 5 NFC costs \$45.

Headquarters: Palo Alto, USA

Duo

[Duo](#) offers several 2FA solutions, including ones that incorporate Yubikey hardware tokens, confirmation requests delivered to the Duo app that foil man-in-the-middle attacks, and time-based one-time passcodes.

Platforms: Duo app is available on Android and iOS

Price: Has a free option. Premium plans begin at \$3 per user per month.

Headquarters: Austin, USA

Other two-factor authentication services

Google Authenticator app: Google offers a free authenticator app that creates time-based one-time passcodes for 2FA purposes. It does not have the same functionality as Duo or a YubiKey. of them offers official mobile apps.

Disk encryption

All your devices should use some form of disk encryption to prevent unauthorized access to your devices' data storage in the event they are stolen or lost. By encrypting your smartphone or computer's hard drive, you turn your sensitive data into illegible code that can only be decrypted by your password. All the options discussed below are examples of disk encryption software.

VeraCrypt

[VeraCrypt](#) is an open source disk encryption service. Using VeraCrypt, your employees can encrypt the hard drive on their device, encrypt their USB flash drive, or even hide how much volume they have on their hard drive.

Platforms: Linux, macOS, Windows

Price: Free

Headquarters: N/A

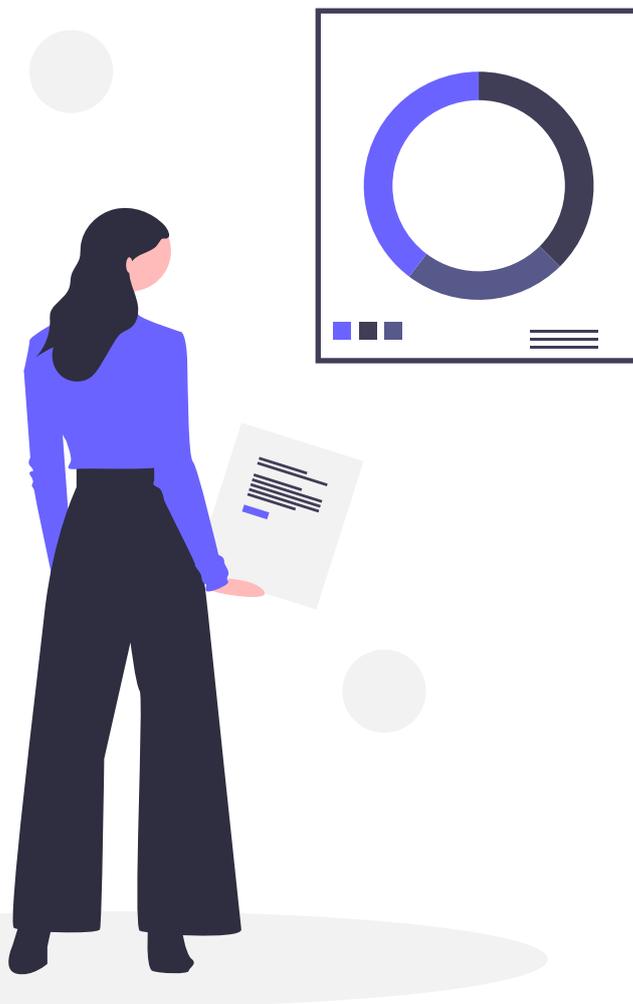
Other disk encryption services

FileVault: [FileVault](#) is available on macOS X Lion and later. You can use it to fully encrypt your startup disk.

BitLocker: [BitLocker](#) is available on most Windows 7 and Windows 10 devices. It is a strong, full disk encryption service.

LUKS: [LUKS](#) is a free, open source hard disk encryption service for Linux.

Native encryption for Android and iOS: Any 3G iOS device or later and any Lollipop (5.x) Android devices or later are equipped with their own native disk encryption services. To learn how to encrypt your Android device, click [here](#). To encrypt your iOS device, click [here](#).



Personal antivirus software

Antivirus software (AVS) is a preventative measure meant to keep your devices clean. AVS scans your device for any malware, from ransomware to rootkits. If it detects any, it will attempt to remove them. More modern AVS also provides malware prevention measures.

Bitdefender

[Bitdefender](#) has strong antivirus protection, but it is light enough that it won't slow your device down. The AVS receives daily updates so that no malware can take it by surprise. They also have a more [advanced option for larger offices](#). It will protect your servers and all your endpoint workstations without bogging down your network.

Platforms: Android, macOS, Windows are available free. iOS is available with a paid plan.

Price: Has a free option. Small office security starts at \$99 for one year for five devices.

Headquarters: Romania

Advanced network security

This is just an introduction to some of the advanced tools for businesses that have their own internal network. These tools will help you secure your network, prevent vulnerabilities from arising, and help you deal with any threats or malware that make it past your defenses. Most, if not all, of these tools will require an IT expert to properly install and configure. If your company does not have its own internal network, these tools are not necessary.

Intrusion detection/intrusion prevention system

An intrusion detection/prevention system (IDS / IPS) monitors your network for malicious activity, policy violations, or malware. If it detects any of these, it will notify your IT admin or send a report to your security information and event management (SIEM) system (more on that down below). Depending on the threat it finds, your IDS / IPS could also attempt to stop the malicious activity.

Snort

[Snort](#) is an open source IDS/IPS that can perform real-time traffic analysis and packet logging on Internet protocol networks. It can also detect a number of probes and attacks and take action to stop them.

Platforms: Fedora, Centos, FreeBSD, Windows

Price: Free

Headquarters: N/A

Suricata

[Suricata](#) is also an open source IDS/IPS that can perform real-time traffic analysis. By using the extensive rules it has built-in, Suricata can scan for complex threats.

Platforms: FreeBSD, Linux, macOS, Ubuntu, UNIX, Windows

Price: Free

Headquarters: N/A

Network scanner

A network scanner searches your system for vulnerabilities in your security. If it detects a weakness in your network, it will send a report back to your IT admin. They will then use this report to address the found vulnerabilities and make the network more resilient.

Nmap

[Nmap](#) is an open source network scanner. In addition to finding network vulnerabilities, you can use Nmap to identify open ports to prepare for a network audit or to generate traffic to hosts on a network and measure their response time.

Platforms: FreeBSD, Linux (all distributions), macOS, Windows

Price: Free

Headquarters: N/A

Security Content Automation Protocol

SCAP is an automated system that will scan your system, searching for vulnerable versions of software. SCAP lets your company benefit from the entire SCAP community of IT security experts. They define the different configurations and use cases that SCAP should look out for, making SCAP a comprehensive patch scanning tool.

OpenSCAP

[OpenSCAP](#) is an open source SCAP system that will make sure your system is conforming to the policies and rules the SCAP community creates. With dozens of different policies, you can find the one that is right for your organization.

Platforms: CentOS, Debian, Fedora, Scientific Linux, Red Hat Enterprise Linux, Ubuntu

Price: Free

Headquarters: N/A

Security information and event management

A SIEM system aggregates all data from your network and then uses rules-based or statistical correlation engines to identify a baseline for what qualifies as normal activity on your network. It then searches for any deviations from this baseline. If it finds something it thinks is not normal, it will take action to stop it. It is also a repository for your IT admin to monitor and search your network records.

Prelude

There are two [Prelude](#) products: Prelude OSS and Prelude SIEM. Prelude OSS is a universal, free, open source SIEM system, but it is meant for smaller networks or for research. The more powerful [Prelude SIEM](#) is available for businesses and to secure larger and more complex networks. Both systems aggregate data from all your IT security tools, regardless of their brand or mark. They will work with either of the two IDS/IPSs on this list.

Platforms: Arch Linux, CentOS, Debian, Fedora, Gentoo, Mageia, Red Hat Enterprise Linux, Ubuntu

Price: The cost of a license for Prelude SIEM depends primarily on the number of devices that send their data to the system, whatever the volume.

Headquarters : N/A

OSSIM AlienVault

[AlienVault](#) is now part of AT&T Cybersecurity, but their open source SIEM system, OSSIM, is still available for free. In addition to letting its users collect and correlate event logs, OSSIM is connected to AlienVault's Open Threat Exchange, which allows users to report and receive updates about the latest malicious hosts. It also works with Snort and Suricata. Be careful because OSSIM [is not a log management solution](#). If that is what you want, you would need to use either [USM](#) (paid version of OSSIM) or another log management system such as Elastic Stack.

Platforms: Must be installed on a virtual machine

Price: Free

Headquarters: San Mateo, USA

Elastic Stack

[Elastic Stack](#), or its previous iteration, [ELK](#) (which stands for Elastisearch, Logstash, and Kibana, the three primary projects), is more of a data visualization system than specifically a SIEM, but it can be used as one. All the products in the stack are open source, and together they let you have a complete picture of your system and your employees' activity.

Platforms: Docker, Linux, macOS, Windows

Price: Free

Headquarters: Mountain View, USA

Network firewall

A network firewall is a network security system that monitors and controls incoming and outgoing network traffic between two or more networks based on a series of predetermined security rules. A firewall typically establishes a barrier between your internal network and other external networks, such as the Internet. A network firewall runs on your network's hardware.

OPNSense

[OPNsense](#) is the open source fork of the [pfSense](#) firewall software distribution. It can be installed on a computer or virtual machine to create a network firewall.

Platforms: HardenedBSD

Price: Free

Headquarters: Middelharnis, The Netherlands

iptables

[iptables](#) allows system administrators to configure tables, chains, and rules in the Linux kernel firewall. This gives the admin control over how data packets enter and travel around the system.

Platforms: Linux

Price: Free

Headquarters: N/A

firewalld

[firewalld](#) is an open source, dynamically managed firewall that allows you to establish different levels of trust around your network. It also works using the Linux system's iptables to filter data packets.

Platforms: Linux

Price: Free

Headquarters: N/A





ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click [here](#).



Accounts

Settings

Help

Close Bridge

ACCOUNT

STATUS

ACTIONS

▼ billporta

● connected

🔌 Log out

🗑️ Remove

➕ Add Account

🔍 Help



CONNECTED



VPN SERVER

US East



IP

69.204.13.205



VPN IP

194.59.251.100

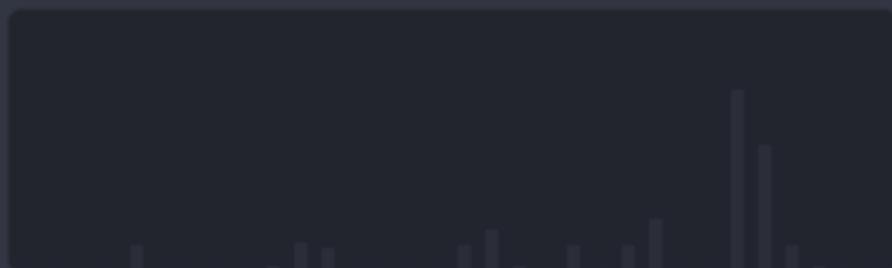


DEFAULT DISPLAY

QUICK CONNECT



PERFORMANCE



↓ 1 kbps

↑ 4 kbps

🕒 04:46

USAGE



Download

741 MB

Upload

87 MB

QUICK SETTINGS



SUBSCRIPTION



Three Year Plan

VPN SNOOZE



-

5:00

+

Snooze



The ProtonMail Guide to IT Security for Small Businesses

Protect your network



The ProtonMail IT security team

Protect your network

READ THIS CHAPTER to identify the IT security best practices your IT security leader should be in charge of, including:

- Network security basics
- Creating a secure internal network
- Maintaining user security
- Log auditing
- Advanced network security
- Data backups
- IT security admin best practices list

Network security sounds complicated, but at its heart, it is straightforward. Similar to how you lock up your office, you must lock up your network to keep your data safe. You must be able to prevent and react to the unauthorized access to and abuse of your network. This requires having technological solutions, documentation, processes, and an IT security leader or admin to control the flow of information over your company's system. While this IT security leader should be able to handle the more technical aspects of network management, their job is impossible unless your staff regularly implements IT security best practices (See Chapter 2).

Your network encompasses all your devices, including computers, laptops, workstations, servers, tablets, or smartphones and all of their connections, either to each other over a local area network or to the Internet. This could be as simple as two laptops sharing documents over the cloud or as complex as companies that have their own internal networks running off private servers.

This chapter gives a basic outline of the responsibilities of your IT security leader and what they should do to maintain your network security.

IT security leader basics

Just as every company handles different data, each company faces unique threats. Precautions that would make sense for one company may not be necessary for another. For example, most small businesses that are not focused on information technology do not need to concern themselves with an internal network or a firewall or a SIEM. Instead, they should focus on taking simple steps that can significantly reduce their business's vulnerability.

Train employees on IT security

The most critical step is training your staff and cultivating a culture of IT security awareness. (See Chapter 2)

Remind employees about phishing attacks and describe new threats

IT security threats are constantly evolving. Hackers are continually exploiting new bugs and creating new types of social engineering attacks. Keep your employees and colleagues up to date by sending out a brief email update on the latest and most popular threats. These updates will help them recognize any hacking or phishing attempts they might encounter.

Conduct a brief assessment of employee adherence to the Employee IT security best practices list

Without regular tests and reminders, even the most conscientious employees can forget about IT security best practices. Conduct a simple test or hold a brief meeting to make sure your employees and colleagues are adhering to IT security best practices. These evaluations or meetings are also an excellent time to address any questions about IT security your employees or colleagues might have.

Create a database of approved devices

But before the training even begins, your IT security leader should create a comprehensive database of all the devices that connect to your company's network or have access to its data. Each one of these devices is a potential weak point. Your IT security leader should ensure that all network-connected devices, including smartphones, are using a firewall and full disk encryption.

Establish permission levels for employees and devices

Once you know which devices will be connecting to your network, your IT security leader should create different levels of access to your company's data, depending on what that employee does. This includes physical access to sensitive network devices and hard-copy files. No employee should have access to portions of data that are not essential to their day-to-day tasks. Only pre-approved employees should be able to download or install new programs on their device.

Use privacy-focused services

Look into replacing software or applications that your business uses to handle sensitive data with privacy-focused services. These types of programs or apps generally use end-to-end encryption (E2EE) to keep information inaccessible except to its owner (and, depending on the service, its intended recipient). Chapter 4 has a comprehensive list of a range of privacy-focused services your business can use.

Creating a secure internal network

As your business grows, you will need to adjust your IT security precautions. Eventually, you will need to start putting in place technological tools, like your own business WiFi network, internal servers, and a firewall. This will also require an IT security leader with more technical expertise

as well.

You should follow the steps below as your business grows. Using a secure WLAN can be done by companies of any size, but implementing a firewall, segmenting your network, or using a corporate VPN only apply to businesses that run their own internal network.

WLAN Security

Nearly every business needs Internet access to handle day-to-day tasks. To be secure, you need to have your own, dedicated WiFi router. All WiFi routers sold since 2006 use the [WiFi Protected Access 2](#) protocol, which is currently the most secure. If you are concerned, check your wireless card or device for a "Wi-Fi CERTIFIED" label to see if it uses WPA2.

The next step is to make sure you use the Enterprise mode of WPA2—also known as 802.11i. This is more complex to set up than a standard WiFi network, but it offers several essential security advantages, the most important of which are the elimination of shared passwords and WiFi snooping.

Set up a network firewall

A properly configured firewall is your internal network's first line of defense. It filters the data of your network or device and only allows permitted traffic through. If your corporate network is connected to the Internet, a perimeter firewall will prevent bad actors from accessing your network by blocking traffic that doesn't meet a predetermined set of criteria.

Segment your network

Segmenting your network is the best way to prevent a full system failure from occurring if a malicious actor or malware make it past your firewall. If your network is segmented, even if one server is compromised, the malware can be contained, and the rest of your IT infrastructure can continue functioning. You should base the decision of how to segment your network on the sensitivity of the data being handled and where the traffic is initiated. A server that is accessible from the Internet should not be located on the same network as a server containing sensitive data.

There are three ways you should think about segmenting your network: using [Network address translation \(NAT\)](#), maintaining separate WiFi networks for employees and guests, and creating virtual local area networks (VLAN).

Your employees' devices should not have their own, public IP addresses. NAT allows several computers on the same network to share one public IP address at the same time. If your company employs a dynamic NAT, you add another layer of protection between your internal network and the Internet, as the NAT will only allow connections that devices from your system initiate.

Your business WiFi network should not be shared with guests. Even with WPA2 Enterprise, allowing untrusted devices onto your WiFi poses the risk of introducing malware into your network. Restricting visitors to a separate WiFi network segment will also prevent them from

accessing internal services, such as network files and printers. Finally, it gives you a greater measure of control over your guests' WiFi without affecting your employees' WiFi.

Finally, make sure your employees' devices and your corporate servers are connected to different VLAN. A VLAN is an example of software-defined network segmentation. It partitions and isolates parts of a single physical network so that network applications can be kept apart.

Use a corporate VPN

A firewall will protect and segment your network, but today, more and more employees are working remotely. You need to find a way for them to securely access your corporate data so that they can do their jobs. This is different from a VPN service that will encrypt your Internet connection. While it will use the same type of protocols (OpenVPN or IKEv2), a corporate VPN creates an encrypted connection over the Internet to your company's corporate server, letting your employees safely download and transmit files without any fear of malicious actors intercepting or manipulating your data.

Advanced IT security leader best practices

Once your company has established its own internal network, your IT security leader's responsibilities will dramatically change, as will the expertise necessary for the job. In addition to keeping your staff trained and up to date, they will have to work much more extensively with the technological tools you have put in place to secure your system.

Maintaining user security

Reassess role-based access management and separation of duties

Companies are not static. New employees come, old employees are promoted, projects end and new ones are reassigned. The turnover of the business cycle means that the type and amount of data that an employee should have access to is continuously shifting. By keeping employees' access limited to only the data they need to perform their day-to-day tasks, you reduce the chance of a catastrophic breach if one account is compromised. Your IT security leader should regularly assess which employees have access to which data and confirm with their supervisor that that level of permission is appropriate. Role-based access control will need to be implemented to define which user is allowed to access which data.

Disable old or obsolete accounts

Old, unused, and inactive accounts are a security threat. Your admin must disable them in a regular and timely manner.

Always check to make sure there is not a reason these accounts have been inactive (like that employee is gone on vacation or parental leave). Also, check to see if any employees have recently been fired or quit, and have them added to the list. Once the list is prepared, and your IT security leader has double-checked it, they should go through and disable user accounts one at a time.

Log auditing

Review security information and system logs (with a SIEM, if applicable)

Every device on your company's network should produce comprehensive event logs that you can search, filter, and review. These logs will help your IT security leader catch any emerging issues or security threats early on.

These reports should all go into a centralized location. By having the reports and records all in place, you can search for abnormal behavior and make sure they are not modified by accident or deleted or altered maliciously.

A SIEM (security information and event management) system aggregates data from

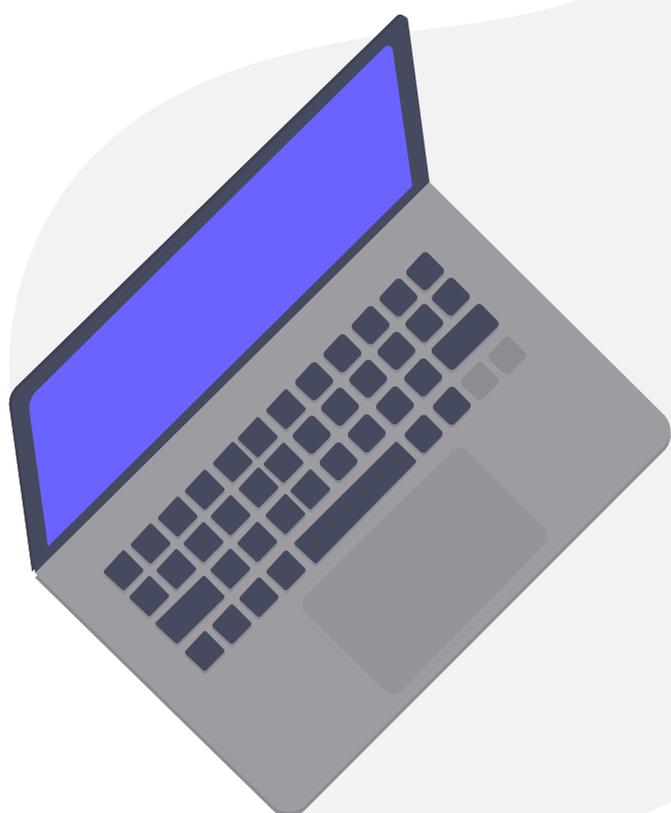
your network and uses rules-based or statistical correlation engines to determine what normal activity on your network looks like, identify any deviations, and take appropriate action. A SIEM system also allows you to view in one place all the logs and records your network generates, making it much easier to spot suspicious patterns. While this is a more advanced tool that should be employed on larger networks, if your company's network does have a SIEM system, check it regularly.

Whether your IT security leader uses a SIEM or manually checks your system's logs, they should do it on a regular basis to make sure nothing unusual has been detected and to make sure the logs are being recorded as expected. If an attack or a failure happens and they do not have any records to go over, it will be difficult to find and solve the problem.

Review user activity and remote access logs

The easiest way to start spotting suspicious activity is by looking at who is logging in and from where. If someone is logging in remotely after you just saw them in the office, or if someone who has been fired has just logged in, there may be foul play involved. Your IT security leader should regularly review these logs, flag all suspicious logins, and follow up by contacting the account owner to find out what they were doing. If the employee is unaware of the login or has reason to think their account may have been compromised, your IT security leader should check to see if any sensitive data was accessed and take measures to ensure the account's security (like changing its password or temporarily suspending the account).

- **Flag any suspicious logins.**
- **Record who was involved, what happened, and when it happened.**
- **Check to see if any sensitive data was accessed.**
- **Take action to secure data/account.**



Advanced network security

Check computer lifecycle and update as necessary

Your list of all network-connected devices must expand to include all your business's servers and workstations. This inventory should be updated anytime new systems or hardware are integrated into your network.

Check software lifecycle and update as necessary

In addition to a list of all your devices and hardware, you should maintain and append a comprehensive list of all the software you are using on them, along with their most recent update. Software updates are often released to fix known bugs. By using an old version of a program, you are introducing a vulnerability into your system. This inventory should be updated anytime software or applications are integrated into your network.

Your IT security leader should also regularly check online to see if there are new versions of any of the programs you are using. If one has been updated, then download the update (or email fellow employees to download the update). Then open up your software inventory and add the details of this update, new program, or application.

Check and install latest security patches (with SCAP, if applicable)

Failing to carry out regular security [patches](#) is one of the most common points of failure in any computer network, and often holes appear as a result of bad processes in systems' maintenance.

SCAP, or the Security Content Automation Protocol, is an automated system that will scan your system searching for vulnerable versions of software. Using SCAP lets your company benefit from the entire SCAP community of IT security experts. They define the different configurations and use cases that SCAP should look out for, making SCAP a comprehensive vulnerability scanning tool.

Test your firewall security

Your IT security leader should regularly check your firewall security to make sure that your company's servers cannot be accessed from the outside through an unknown port.

They should run a scan to make sure the only ports on your network that are open are the ones they have whitelisted. Perform an external to internal [port scan](#) with Nmap.

- **Check which ports are supposed to be opened.**
- **Perform a remote scan with Nmap and compare the result.**

Evaluate firewall configuration

If the firewall security test did not perform as expected, then your IT security leader should evaluate the firewall configuration.

To make sure the firewall is configured properly, your admin should look at the different settings your firewall offers and adjust them to resolve the issue you found. To do this, they will need to also validate the authorized flow of traffic into your system as well as between internal zones (if applicable).

They should go through the sub-checklist below to troubleshoot the basic settings that might have caused the firewall security test to fail.

- **Check anti-spoofing filters.**
- **Check user permit rules.**
- **Check system administrator alert settings.**
- **Check system traffic log analysis.**

Test and run antivirus software

Antivirus is a preventative measure. It works to detect, quarantine, and remove any known malware that makes it on to your system. Ideally, your network will not be flooded with malware, and so it may be hard to know if your antivirus is doing its job sometimes. But given the essential role antivirus software plays in your overall network security, and especially for workstations or servers dealing with files, it is crucial your IT security leader tests your

antivirus software regularly.

They can test the resilience of your antivirus software by downloading an EICAR file designed to simulate a virus or malware infection. EICAR files are completely safe and used by IT security experts to see if antivirus programs are working as they should.

Follow the process in the sub-checklist below.

- **Download the EICAR file.**
- **Run an isolated scan for the EICAR file.**

Your system's antivirus software should detect the EICAR file, alert you, and quarantine it. If it does not, you should strongly consider getting new antivirus software.

Following the EICAR test, perform a full system scan:

- **Launch your antivirus software control panel.**
- **Perform a full system scan.**
- **Isolate and quarantine any threats detected.**

Data backups

Making backups of your business's data is not necessarily part of network security. It is more like your insurance policy in case your network security fails. If ransomware compromises your company's devices or if there is a system failure, these backups will help your company get back on its feet.

Check and back up system data

Your IT security leader needs to make regular backups of all your most vital data. Remember, it is better to be over-inclusive than for a system crash to halt your business because you did not save the correct folder. Ideally, the backup process will be automated.

Even if the backup process is automated, your admin needs to regularly verify that all the processes are running smoothly and that the data are actually being saved.

- **Ensure servers are fully backed up.**
- **Ensure workstations are fully backed up.**

Making sure the backups are working and accessible is just as important as checking to make sure the data are being backed up in the first place. Using a random sample of files from the most recent backup, your IT security leader should try opening them on a workstation machine to see if the data are accessible. You should test at least three backup files to get a more reliable result.

- **Take three backup images made in the last week.**
- **Load them all onto the same configuration as their parent system.**
- **Check they are all working as expected.**

Evaluate backup process

If the backup files your IT security leader tested were inaccessible or corrupted, they must now locate the problem in your automated backup system. Finding the problem can require extensive testing at each stage of the automatic backup process, including re-saving and re-testing system-wide backup files or changing to a new automated backup process.

- **Perform backup process troubleshooting.**
- **Test three more random backup samples.**
- **Evaluate your current backup process.**
- **Consider changing to a new backup process.**





ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click [here](#).

NOTICE: THIS APPLICATION IS FOR CLAIMS-MADE AND REPORTED COVERAGE. READ THE ENTIRE APPLICATION CAREFULLY.

I. APPLICANT INFORMATION

Name of Applicant: _____
 (Include names of all subsidiary or affiliated companies to be insured, or attach separate sheet, if necessary)

Principal Address: _____

City: _____ State: _____ Zip Code: _____

Mailing Address (if different): _____

City: _____ State: _____ Zip Code: _____

Telephone Number: _____ Fax Number: _____

Email: _____ Corporate Website Address: _____

II. COVERAGE REQUESTED

Requested Effective Date: _____

III. YOUR BUSINESS

1. Nature of business: _____

2. Description of operations: _____

3. Total annual revenues (indicate complete number, e.g., \$1,000,000): _____

4. Estimate total number of customer and/or employee records stored by you or by third parties on your behalf, either electronically or in physical files.

- 0-100,000
- 100,001-250,000
- 250,001-500,000
- Over 500,000
- I don't know

5. Does the Applicant use anti-virus software and a securely configured firewall to protect its network? Yes No

6. Does the Applicant utilize a cloud provider to store data? Yes No

If "Yes", please name the cloud provider: _____

If the Applicant utilizes more than one cloud provider to store data, please name the cloud provider storing the largest quantity of customer and/or employee records, including medical records, personal health information, social security numbers, bank account details, and credit card numbers.

For Question 7, if the answer is "No", PCI DSS Liability coverage will not be available.

7. Are you (or your credit card point of sale vendor, if applicable) PCI-DSS Compliant? Yes No

IV. LOSS HISTORY

If the answer to any of questions 8-10 is "YES", please provide specific details on a separate page.

- 8. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:
 - a) Received any complaints or demand letters, or been the subject of any litigation, government action or investigation, or other regulatory or legal proceedings involving matters of privacy injury, breach of private information, violation of privacy law, network security, identity theft, denial of service attacks, computer virus infections, theft or loss of confidential information, damage to third party networks, or the ability of third parties to rely on the Applicant's network? Yes No
 - b) Sustained any unscheduled network outage or interruption for any reason? Yes No
 - c) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? Yes No
- 9. Does the Applicant or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach or other privacy-related event or incident, cyber extortion demand or threat, or allegations of breach of privacy? Yes No
- 10. Has any IT service provider that the Applicant relies on sustained an unscheduled network outage or interruption lasting longer than 4 hours within the past 3 years? Yes No
 If "Yes", did the Applicant experience an interruption in business due to such outage or interruption? Yes No

V. ACKNOWLEDGEMENTS AND REPRESENTATIONS

1. **The undersigned represents that the statements, representations and information contained herein, or attached to this Application, are true and complete, and that reasonable efforts have been made to obtain sufficient information to facilitate the proper and accurate completion of this Application.**
2. **The undersigned acknowledges that the signing of this Application does not bind the undersigned to complete the insurance. The undersigned further acknowledges that the statements, representations, and information contained herein, or submitted with this Application (which shall be retained on file by the Underwriters and shall be deemed attached hereto, as if physically attached hereto), are material to the risk assumed by the insurer; that any policy will have been issued in reliance upon the truth thereof; and that this Application and all written statements and materials furnished to the Insurer in conjunction with this Application shall be deemed incorporated into and made a part of the policy, should a policy be issued.**
3. **Underwriters hereby are authorized to make any investigation and inquiry in connection with this Application as they may deem necessary.**
4. **The undersigned acknowledges and agrees that if the information supplied on this Application, or in any attachments, changes between the date of the Application and the effective date of the policy period, the Applicant will immediately notify the Underwriters of such change, and the Underwriters may withdraw or modify any outstanding quotations and/or agreement to bind the insurance.**
5. **For purposes of creating a binding contract of insurance by this Application, or in determining the rights and obligations under such a contract in any court of law, the parties acknowledge that a signature reproduced by either facsimile or photocopy shall have the same force and effect as an original signature, and that the original and any such copies shall be deemed one and the same document.**

Signed: _____ Print Name: _____

Must be signed by an authorized officer, partner or principal of the Applicant

Title: _____ Date (Mo/Day/Yr): _____

Applicant Organization: _____

Please Return to: greg.cooke@usi.com or fax to 610.537.2743

The ProtonMail Guide to IT Security for Small Businesses

Enforce email security



The ProtonMail IT security team

Enforce email security

READ THIS CHAPTER to understand the email security best practices regarding:

- Phishing attacks
- Imposters spoofing your email
- Email security best practices list

Email security is vital to your business's overall IT security because it is the most common attack vector. Phishing emails and fraud are two attacks that do not require any technical skill, merely an understanding of human nature, a flair for deception, and an email address. Fooling a human into clicking on a malicious link is a much easier way to penetrate a network than trying to hack its firewall.

Phishing and fraud are becoming ever more extensive problems. [A recent threat survey from the cybersecurity firm Proofpoint](#) stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI [reported](#) that these types of attacks cost companies around the world \$12 billion annually.

Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This

must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.

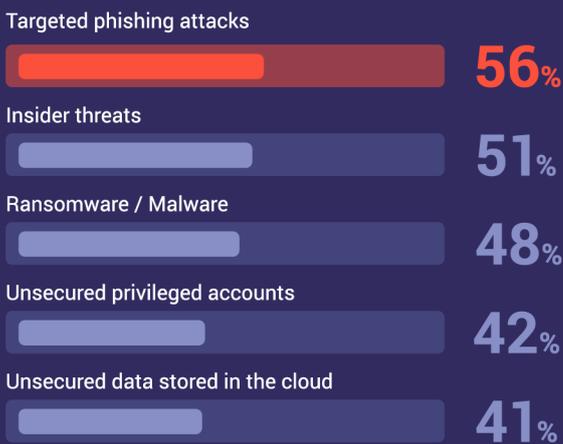


Receive an email? **DON'T GET PHISHED**

Phishing is a type of cyberattack in which a hacker, pretending to be a trusted individual or organization, tricks the victim into opening a malware-containing email.

This can have terrible consequences for your business, including loss of confidential data, leak of financial information and identity theft of your employees' data.

The greatest security threats faced by organization:



Phishing attacks are the most pressing cyber security challenge



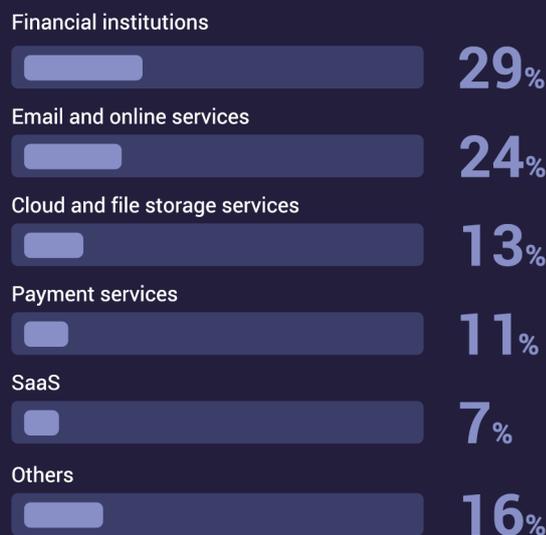
Source:
Cyberark, IT security professional respondents, multiple responses allowed

83% of global infosecurity respondents experienced phishing attacks in 2018



Source: "State of the Phish Report"

Top phishing targets by industry:



Email remains the most popular method of phishing attack



Phishing

Phishing is by far the most common type of IT security threat your business will face. It involves someone posing as a legitimate customer, institution, or colleague to fool your employees into sharing sensitive data, such as business financial details and passwords, or clicking on a malicious link that will compromise their device.

Phishing takes many different forms. Recently, it was reported that [Google and Facebook were scammed out of over \\$120 million](#) by someone who sent forged contracts and invoices asking for payment. Or, in what is probably the most infamous example of phishing, the campaign manager of Hillary Clinton's presidential bid was [fooled into clicking on a malicious link and entering his Google password](#). This exposed his entire Gmail inbox.

Phishing can also involve texts and instant messages, but given email's ubiquity, it is by far the most common medium.

How to prevent phishing

Training

Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. This training should be continuous as well. Phishing attacks are always evolving.

Create a process

Your business will receive phishing emails. So eventually, someone will fall for one. If this happens, your company needs to have a process in place that everyone knows and understands. An employee must know whom to speak with if they think they were just phished. By acting swiftly, you can mitigate the damage of a phishing attack.

Limit public information

Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories, including phone numbers or physical addresses. All these pieces of information can help attackers engineer an attack.

Carefully check emails

First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the "From" address to see if it is odd (e.g., service145@mail.145.com). If an email looks suspicious, employees should report it.

Beware of links and attachments

Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. Attachments are especially dangerous because they may contain malware, such as ransomware or spyware, that can compromise the device or network.

Do not automatically download remote content

Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it.

Never share sensitive information without being sure who is on the other end

No organization should EVER ask for your password via email. If an email is asking you to send your password, credit card number, or other highly sensitive information in an email, this should be a red flag.

Hover over hyperlinks

Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL. You can retrieve the original URL [using this tool](#).

If in doubt, investigate

Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email.

Take preventative measures

Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims

to come from, making it easier to identify potential phishing attacks.

What to do if your company is phished

Follow your company's procedures

Your company must have a process in place for employees who think they may have been fooled by a phishing email. The first step should be reporting the phishing email and any data that was shared to your organization's IT security leader.

Limit the damage

Once your organization understands what the phishing attempt looked like and what information was exposed, your IT security leader should immediately change the compromised passwords. It may also be necessary to disconnect that employee's device from the network to prevent the spread of malware.

Alert others

Your IT security leader should also warn the rest of your employees that there has been a successful phishing attempt and tell them exactly what to look for. Once a phisher sees success with one employee in an organization, they'll often target others to increase their access. You should also inform the company or person that was impersonated that their identity is being used in a phishing scheme.

Notify customers if necessary

If the data exposed affects your clients, make sure you notify the affected parties — they could be at risk of identity theft.

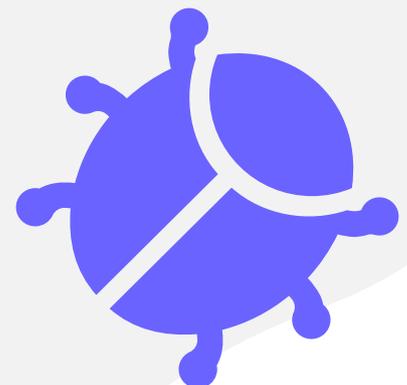
Notify authorities

American businesses should report phishing attacks to the local law enforcement, the FBI's Internet Crime Complaint Center at [IC3.gov](https://www.ic3.gov), and the FTC at [FTC.gov/Complaint](https://www.ftc.gov/Complaint). You can also forward phishing emails to:

spam@uce.gov (an address used by the FTC) and to **reportphishing@apwg.org** (an address used by the Anti-Phishing Working Group).

Imposters spoofing your email

This is when an attacker sets up an email that is identical to your business email address and sends out phishing attacks that appear to originate from your company. This degrades the trust your vendors and customers have in your company.



How to prevent your email from being spoofed

Use email authentication

This type of technology allows a receiving server to verify that an email you sent actually came from your company. This makes it much more difficult for scammers to impersonate organizations.

Domain-based Message Authentication, Reporting, and Conformance, or DMARC, is one of the primary ways to detect spoofed emails. DMARC can also be configured so that you are alerted anytime someone receives an email that appears to be a spoof of your domain.

ProtonMail also has advanced security features, like [Authentication Logs](#), [Encrypted Contacts](#), and [Address Verification](#). Authentication Logs allows you to monitor if anyone else has logged in to your account. If you detect another user on your account, or an active session on a device you don't control, you can remotely log out. Messages sent between ProtonMail accounts are only vulnerable if a hacker compromises the end-user or stages an elaborate man-in-the-middle attack. Encrypted Contacts and Address Verification make it much more difficult for these types of attacks to succeed. These advanced features make it harder for anyone to access, tamper with, or impersonate your emails without your knowledge.

Keep your programs and apps up to date

A hacker could also access your emails through a compromised network. Always keep your security patches up to date and continually update your apps and programs so that you are using the latest version. Ideally, you should set them to update automatically.

What to do if your email is spoofed

Notify customers

If you discover that hackers are spoofing your business's email and using it for phishing attacks, you must tell your customers as soon as possible — by mail, email, or social media. You should inform your customers what your legitimate emails look like, what types of information your company will and will not request, and any other information they can use to spot phishing emails.

Notify authorities

American businesses should report spoofed emails to the local law enforcement, the FBI's Internet Crime Complaint Center at [IC3.gov](https://www.ic3.gov), and the FTC at [FTC.gov/Complaint](https://www.ftc.gov/Complaint).

References

Page 2: **1.** Knowbe4, 2018 **2.** FBI, 2017 **3.** PhishLabs, 2019, Phishing Trends & Intelligence Report: The Growing Social Engineering Threat **4.** Symantec, Symantec Internet Security Threat Report-2018, 2018



ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click [here](#).

BitLocker

01/25/2018 • 7 minutes to read •  +5

Applies to

- Windows 10

This topic provides a high-level overview of BitLocker, including a list of system requirements, practical applications, and deprecated features.

BitLocker overview

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

On computers that do not have a TPM version 1.2 or later, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation. Starting with Windows 8, you can use an operating system volume password to protect the operating system volume on a computer without TPM. Both options do not provide the pre-startup system integrity verification offered by BitLocker with a TPM.

In addition to the TPM, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device, such as a USB flash drive, that contains a startup key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is presented.

Practical applications

Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software-attack tool against it or by transferring the computer's hard disk to a different computer. BitLocker helps mitigate unauthorized data access by enhancing file and system protections. BitLocker also helps render data inaccessible when BitLocker-protected computers are decommissioned or recycled.

There are two additional tools in the Remote Server Administration Tools, which you can use to manage BitLocker.

- **BitLocker Recovery Password Viewer.** The BitLocker Recovery Password Viewer enables you to locate and view BitLocker Drive Encryption recovery passwords that have been backed up to Active Directory Domain Services (AD DS). You can use this tool to help recover data that is stored on a drive that has been encrypted by using BitLocker. The BitLocker Recovery Password Viewer tool is an extension for the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in. By using this tool, you can examine a computer object's **Properties** dialog box to view the corresponding BitLocker recovery passwords. Additionally, you can right-click a domain container and then search for a BitLocker recovery password across all the domains in the Active Directory forest. To view recovery passwords, you must be a domain administrator, or you must have been delegated permissions by a domain administrator.

The ProtonMail Guide to IT Security for Small Businesses

Create a culture of IT security



The ProtonMail IT security team

Create a culture of IT security

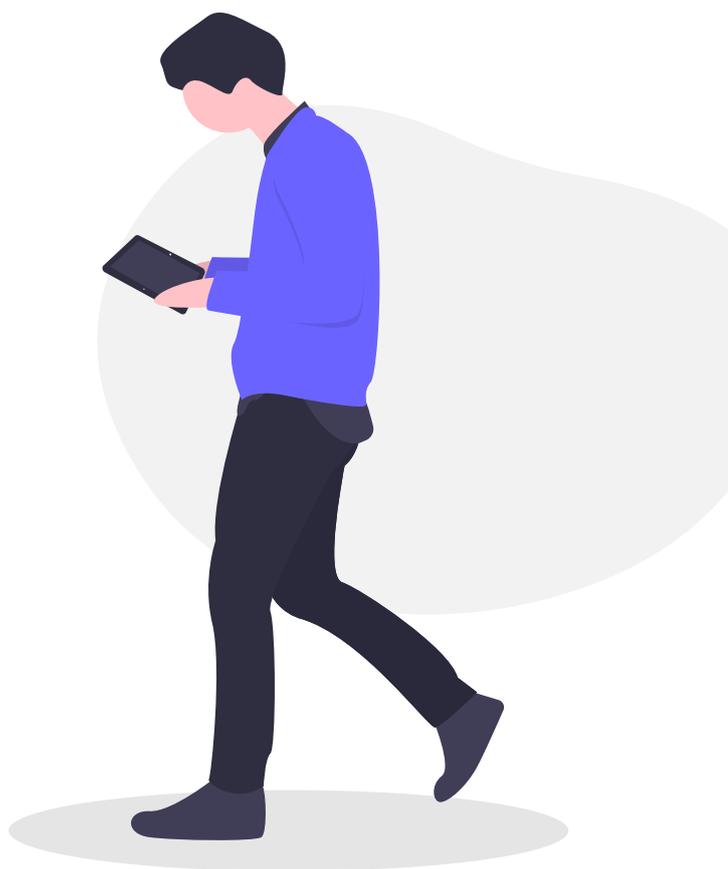
READ THIS CHAPTER to identify the IT security best practices for:

- Laptops and computers
- Smartphones
- Passwords
- USBs
- Employee IT security best practices list

Small business IT security is often overlooked, either due to a lack of expertise or funding. This is a mistake. Data breaches are costly to mitigate but potentially more costly to recover from after they occur. But not all data breaches are the result of a malicious attack by a hacker. Statistically speaking, there is someone that is an even bigger risk to your data than a hacker: your employees.

At least until the robots take over, your business will employ and rely on other human beings. They can be your best defense against cyberattacks — or your most significant vulnerability. Training your staff on basic IT security practices is a good start, but it is not enough. You must emphasize the importance of IT security and turn it into part of the office culture so that employees do not think of IT security as a one-off task, but rather

as part of their daily routine. This chapter will help you identify the necessary steps that your employees should all implement.



Humans are the **WEAKEST LINK**

Employees are your company's biggest asset, but they can also be a hacker's key to your company's confidential information.



It only takes one victim

96%

Email remains the favorite channel for hackers, with 96% of all phishing and social engineering

Small organizations

In 2018, employees of small organizations were more likely to face email security threats – including spam, phishing, and emailed malware – than those in large organizations.

How was the ransomware unleashed?



- 43% Phishing/social engineering
- 30% Insecure/spoofed website
- 15% Malvertisements
- 8% Social media
- 4% Other

Will your team spot the threat?

Ransomware is also a significant concern. According to the Ponemon Institute, more than 4,000 ransomware attacks occur every day in the US alone.

Cybersecurity experts reported that most ransomware programs are unleashed after employees fall for phishing or social engineering attacks.

Malicious email rate by organization size

Organization size	Malicious email rate
1-250	1 in 323
251-500	1 in 356
501-1000	1 in 391
1001-1500	1 in 823
1501-2500	1 in 440
2501+	1 in 556

IT security: neither impossible nor impractical

When people hear the words “IT security” their eyes often glaze over: they assume it is an impossibly technical subject and, therefore, too complicated for them to understand or have any impact on. While explaining how a TLS handshake works is very complicated, that level of knowledge is not necessary. **You can profoundly improve your IT security through relatively simple behavior changes.**

The measures you put in place will depend on the **Threat Model** you developed. The important thing is that these IT security choices are made after a deliberative process in which the risks and rewards are weighed. While the following steps represent basic best practices, not every step will be appropriate for every business.

With that caveat out of the way, let’s jump into measures you should take to secure your company’s data.

Your IT security leader

As part of devising your IT security policy, you designated an IT security leader to train your employees on IT security best practices and ensure those practices are regularly implemented. Your IT security leader must also be prepared to answer any questions your employees may have about how to protect their devices or the data they work with.

It is this individual’s responsibility (with your support, of course) to cultivate a culture of IT security in your office. To create a culture of IT security awareness and keep best practices at the front of your employees’ minds, your IT security officer will need to assess their IT security performance regularly.

Laptops and computers

If your business works with data, most likely that means that your employees either work on computers you supply or use their own laptops. In either case, making sure these devices are secure is vital to your overall **Network Security** (see Chapter 3).

Keep your operating system and software up-to-date

New security flaws are discovered in software every day, which companies fix in the updates they release. However, if you do not actually install the updates, then your device is not secured against these known threats, making it a tempting target. The best solution is to set your device to update automatically.



Windows

For Windows devices: In Windows 10, all updates are done automatically. Press **Windows Key + C** and select Settings. Once the Settings window opens, select **Update & Security**. This

will automatically take you to the Windows Update page. Here, you can see whether you have any updates pending. By clicking **Change active hours**, you can set the times for when your device will attempt to update itself.



Apple

For macOS devices: In macOS 10.6 and later, go to Apple Menu and click **System Preferences**.... Once the System Preferences window opens, click **Software Update**. Once the Software Update window opens, click the box next to Download important updates automatically (for Mac OS 10.7 users, this will read Download updates automatically). From the Check for updates: drop-down menu, you can choose how often you would like to check for updates. We recommend you pick **Daily**.

Enable a local firewall to block incoming network connections

A firewall examines traffic from your network (see Chapter 3) or the Internet, determines what is good traffic, and lets it pass while blocking all the rest. Enabling the firewall on your device prevents intruders from getting unauthorized access to your device.



Windows

For Windows devices: In Windows 10 and later, press **Windows Key + C** and select Settings. Once the Settings window opens, select **Update**

& Security. This will automatically take you to the Windows Update page. Click **Windows Security**. Once the Windows Security window opens, click **Open Windows Defender Security Center**. A new window will open. Click **Firewall & Network Protection**. Here, you can see whether the firewalls for your domain, private, and public network are on.



Apple

For macOS devices: In macOS 10.6 and later, go to **Apple Menu** and click **System Preferences**.... Once the System Preferences window opens, click **Security & Privacy**. Once the Security & Privacy window opens, click on the **Firewall** tab. Then, click on the lock icon in the bottom left corner of the window. You will need to enter your administrator password. Click Turn On **Firewall**.

Enable full disk encryption

Full disk encryption applies encryption to your entire hard drive. This protects your files, pictures, software, and programs from being accessed if your device is stolen or lost.



Windows

For Windows devices: Some **Windows** devices automatically encrypt your disk, others don't, which makes it complicated. To check on Windows 10 and later, press **Windows Key + C** and select **Settings**. Once the Settings window opens, **select System**. Once the System window opens, select the **About** tab. In the About window, scroll to the bottom. If your device enables full

disk encryption, you will see an option to turn off Device Encryption. If you do not see it, you will need to download Veracrypt, which will encrypt your Windows 10 PC's system partition for free.



Apple

For macOS devices: In macOS 10.6 and later, go to **Apple Menu** and click **System Preferences**.... Once the System Preferences window opens, click **Security & Privacy**. Once the Security & Privacy window opens, click on the **FileVault** tab. Then, click on the lock icon in the bottom left corner of the window. You will need to enter your administrator password. Click **Turn On FileVault**. The next screen will display the disk's recovery key. If you forget your password, this is the **ONLY** way to recover the data on the encrypted disk. Please write this 24 character string down and save it in a secure place. Click **Continue**. The next screen will ask if you wish to store your recovery key with Apple. For security's sake, we advise you to select the button labeled **Do not store the recovery key with Apple** and click **Continue**. You will then be prompted to restart your device to enable FileVault and begin encrypting the disk. Click **Restart**. Once you log back in, your device will encrypt the disk in the background.

Only install the software you need; and then, only from trusted sources

The fewer programs a device has on it, the fewer opportunities there are for something to go wrong. Your work computers should be kept

lean, with only the applications necessary for work and your day-to-day tasks. Each of these programs should have been downloaded or purchased from trustworthy sources.

Uninstall software you don't use

A coda to the previous best practice. If there is a program on your device that you never use, uninstall it. That is one fewer program you need to keep updated.

Keep Bluetooth turned off unless you are using it

Bluetooth allows you to link your computer to nearby devices. This is extremely useful if you are trying to share files from your computer with someone. However, these networks also allow intruders easy access to your device. For this reason, they should always be turned off unless you are actively using them.

Do not share access to your device

This is security 101, but no one should be able to access your device. If you do need to share your device with someone, it must be a trusted individual and, ideally, it will be under your supervision. After you no longer need their assistance, you should change your login password.

Be aware of “shoulder surfing”

Penetrating a computer’s defenses is not necessary if you are broadcasting sensitive information on your screen. If you are handling sensitive data, be aware of your surroundings and potential spies looking over your shoulder.

Lock your notebook whenever you step away

All these steps will be completely undone if you leave your device unlocked and unsupervised. An unlocked device is an invitation to any intruder to the data on your device as well as your network. Even if you’re just grabbing a coffee, lock your computer.

Use a VPN on an unknown WiFi network

If you work from home or while you are traveling, you should use a trustworthy VPN service to encrypt your Internet connection. Unknown WiFi networks and public hotspots present all types of security vulnerabilities that can be avoided with a VPN.

Use antivirus software and set up periodic scans

Antivirus software will help you identify and remove any malware that gets on your system. It is an essential part of keeping your device clean and free of malicious programs. Windows 10 comes with antivirus software already installed,

called Windows Defender Antivirus. To access it, press **Windows Key + C** and select **Settings**. Once the Settings window opens, select **Update & Security**. This will automatically take you to the Windows Update page. Click Windows Security. Once the **Windows Security** window opens, click **Open Windows Defender Security Center**. A new window will open. Click **Virus & Threat Protection**. Here you can run a system scan or adjust the settings of Windows Defender.

Use Acrobat Reader with Protected View mode to access PDFs

Hiding malware in PDF attachments is becoming one of the more common ways hackers deliver malware onto a system. Therefore you must be careful anytime you are opening a PDF file. Acrobat Reader has enabled its Protected View mode by default. When a PDF file is opened in Protected View, all the operations Acrobat Reader needs to run to display the PDF are run in a restricted manner inside a confined environment. That way, if there is a malicious program hidden in the file, it is contained and cannot infect your device.

Smartphones

As more and more business is handled remotely, our smartphones are becoming more and more integral to our work — and therefore, to cybersecurity. While it is easy to overlook smartphones, they often have the same access to sensitive data and corporate networks as work computers.

Keep your mobile phone operating system and apps up-to-date

Same as your computer, the software makers for smartphones are continuously finding flaws and putting out fixes in the form of updates. If an app or your operating system has not been updated recently, your device could be vulnerable to exploitation.

Enable full device encryption

Since we take our smartphones with us everywhere, they are much more likely to be lost or stolen than a computer. Now that smartphones have more storage than some early computers, they could potentially expose a significant amount of data. Encrypting your device will protect the information on your device unless it is unlocked.



Android

To encrypt your Android device, tap Settings and then Security (remember, the phrasing on each Android device might be slightly different). Here you will see the option to encrypt your phone. (NOTE: the encryption process can take over an hour, and your phone has to be plugged in.) Once your phone has been encrypted, you will have to enter your PIN or passphrase to decrypt the data each time you restart the phone.



Apple

The latest iPhones (any after the 3GS) and all iPads automatically encrypt the device's data, but you must set a passcode. For devices running iOS 9 or later (remember to **keep your operating system up-to-date!**) tap **Settings** and then tap **Touch ID & Passcode**. You will then be prompted to create a six-digit passcode. Once your passcode is created, scroll to the bottom of the Touch ID & Passcode screen. You should see a message saying "Data protection is enabled." This means that your device's encryption is tied to your passcode and only your passcode can unlock the data on your phone.

Set a strong PIN code or passphrase

Despite the many advances in ID verification technology, PINs and passphrases are still your most secure option. Biometric methods, like fingerprint or face scanners, are not always protected by law, which means a law enforcement officer could force you to unlock your phone. People rarely make their pattern lock complex enough for it to be secure, and it is easier for someone to figure out your pattern from looking over your shoulder. Androids allow you to make passwords (or passphrases – more on that below) of up to 16 characters, and iPhones and iPads enable you to make alphanumeric passcodes, combining letters, numbers, and symbols. Experts suggest using a passcode of at least eight characters, and those characters should be a mix of numbers, capital letters, and lowercase letters.

Limit the information accessible from the lock screen

Certain apps send updates that you can read without having to unlock your phone. Same for text messages. This means that your passcode does not protect this information. If your device is stolen or lost, an intruder will be able to read the texts you receive even if they cannot access the rest of the data on your phone.



Android

To adjust the notification settings on your Android device, tap **Settings** and then **Notifications**. Then by tapping on each app, you can decide what information they show while the device is locked.



Apple

Adjusting the notification settings on your iPhone or iPad is slightly trickier. For apps that come with the phone (like the Calendar) tap **Settings** and then **Control Center**. Then tap **Access on Lock Screen** to turn the option off. To stop your text messages from being displayed on the lock screen, tap **Settings**, then **Notifications**, then **Messages**. On this screen, tap on **Show on Lock Screen** to turn the option off. To prevent apps from sharing data on the lock screen, you must turn each one off individually by tapping that app's entry in the Notifications screen.

Disable your Voicemail unless you absolutely need it

Voicemails are typically only protected by a four-digit PIN, leaving them vulnerable to being bruteforced. Once an attacker has access to your voicemail, they can request a password reset over the phone number at times when they think you are unlikely to answer. If you miss the call, the reset code will be recorded in your compromised voicemail and the attacker can use it to access your account and lock you out. This also bypasses two-factor authentication. The best defense against this is to shut down your voicemail. If this is not an option, then use the maximum amount of allowable characters for your voicemail PIN, make sure the code is random, and do not use your phone number or phone calls for password resets.

Do not share access to your device with anyone

Any time you share your device with someone else, you are increasing the odds of the device being compromised or your login credentials being shared. If you need to share your device, share it only with someone you trust and, ideally, supervise them. Once they are finished with your device, you should change your passcode

Keep Bluetooth and NFC turned off unless needed

Bluetooth and near field communications (NFC) allow your devices to link and share information with other nearby devices. This is extremely useful if you are trying to share files from your phone with someone. However, these networks also allow intruders easy access to your device. For this reason, they should always be turned off unless you are actively using them.

Passwords

Passwords are the keys to an account. They are a free, simple, and effective way for your employees to prevent unauthorized access to their devices or accounts — provided they use strong, unique passwords.

Use unique, strong (at least 16 characters) passwords for every account

A strong password is one that is unlikely to be cracked or guessed, which means that items like your birthday, your address, or the word “password” should be immediately dismissed. To be strong enough to avoid being cracked by a computer, a password should be at least 16 characters. An alternative to using a password is to use a passphrase. These are more memorable. We advise using a passphrase of at least four obscure words with numbers and characters mixed in. A passphrase like “llama9cakeenn!uilima” is extremely difficult

for a computer to crack because it contains a large amount of entropy. But it is easier for a human to remember because it is only four words (“llama”, “cake”, “ennui”, and “lima”) with two extra characters, the placement of which can be memorized.

Just like you do not use the same key for every lock, you should not use the same password for every account. If you use unique passwords for every account, then even if one password is cracked, the rest will remain secure.

Finally, your passwords should never be written down or out in the open where anyone could access them.

Use a password manager

While passphrases will help make your passwords more memorable, eventually you will have too many accounts to possibly remember a strong, unique password for each. At this point, you should start using a password manager. A password manager securely stores and auto-fills all the passwords for your accounts and thus could also protect you from phishing attack. They can even assist you in creating strong passwords for new accounts. To access these passwords, you type in a single, master password. This way, instead of remembering dozens of passwords, you remember one and your password manager remembers the rest.

Use 2FA wherever possible

Two-factor authentication adds an extra identity verification to the standard login procedure. Instead of just typing in your username and

password to sign in, 2FA requires you to provide another type of credential (a second factor) before you can access your account.

The secure types of 2FA use a time-based, one-time password that is generated by a zero-trust app, such as [Authy](#), [DuoMobile](#), or [Google Authenticator](#), or a physical fob, such as [Yubikey](#).

Store your 2FA codes in a secure place

Each time you set up 2FA on an account, that account will provide you with a set of one-use codes that you can use to log in to their service in case you cannot, for whatever reason, enter the correct form of second verification. These codes need to be stored in a safe, easily accessible place so that you have a backup and can open your accounts even if you have lost your phone or Yubikey fob.

USB peripherals

USB flash drives are a convenient way to store and share data, but they must be treated with caution. Because it is impossible to know what is on them without plugging them in, that makes them ideal vehicles to deliver malware onto devices.

Do NOT use unknown USB devices or sockets

Just like you would not stick an unknown substance into your mouth, you should never

plug an unknown USB drive into your computer. If you do, you let an intruder bypass your firewall and get direct access to your device. If you find a USB drive, give it to a member of your IT team or a tech expert so that they can scan it.

This same caution should be used for USB sockets as well. If you do not know who is in charge of running a public USB socket, like the ones you see at charging stations, you should not plug your device into it. These sockets can also directly access your device.

These best practices will protect you only if they are implemented 100% of the time. This requires creating a culture of IT security awareness.

The most important thing to remember is that creating a workplace culture of IT security awareness requires buy-in from employees at every level. If management doesn't view IT security as a priority, then lower-level employees won't either.

References

Page 2: **1.** CyberArk, Global Advanced Threat Landscape Report 2018 **2.** Symantec, Internet Security Threat Report, 2019 **3.** Symantec, Internet Security Threat Report, 2017 **4.** Verizon, 2018 Data Breach Investigations Report, 11th edition.



ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click [here](#).

Wall Street Journal **Forbes** New York Times Huffington Post

"An alternative to the ad-based revenue model of free services like Gmail which actively scan your emails to deliver relevant ads to you online"



WALL STREET JOURNAL

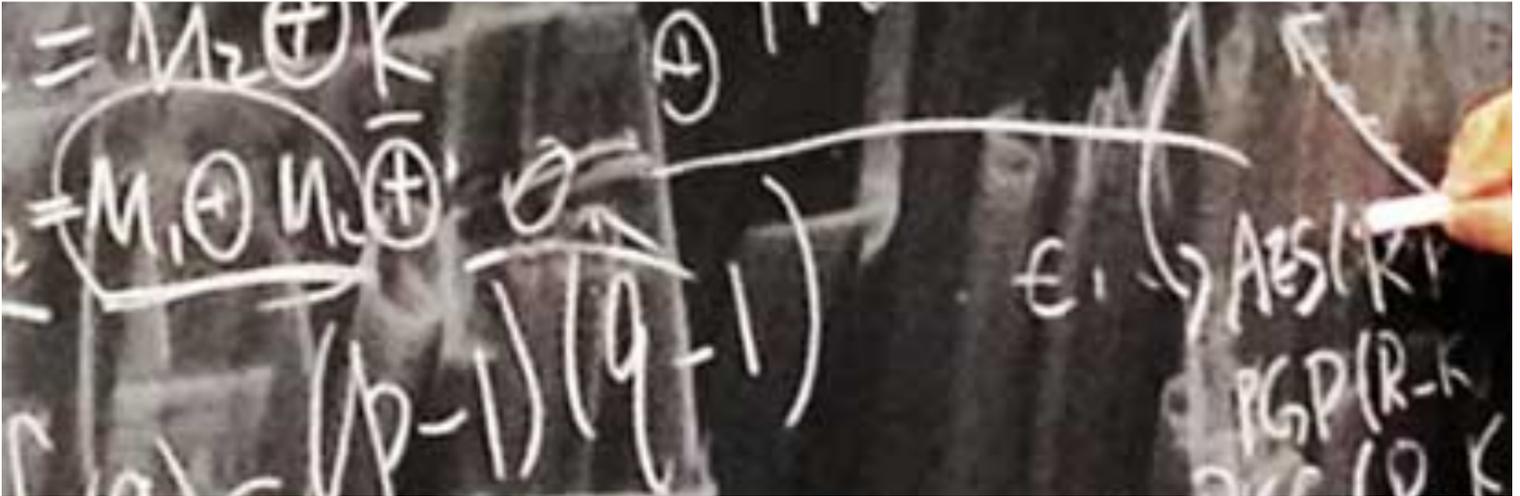
The New York Times

theguardian

Forbes

Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND

FOX NEWS



Our story begins where the web was born, at CERN.

We are scientists, engineers, and developers working to protect civil liberties online.

ProtonMail was founded in 2013 by scientists who met at CERN and were drawn together by a shared vision of a more secure and private Internet. Since then, ProtonMail has evolved into a global effort to protect civil liberties and build a more secure Internet, with team members also hailing from Caltech, Harvard, ETH Zurich and many other research institutions.

Today, we help our community of millions of users secure their private data online. More than 10,000 supporters have assisted us in this mission by donating to make this project possible. Thanks to your support, we are continuing to develop state of the art email privacy and security technology from our home base of Geneva, Switzerland.

Meet our team

Join us



How Sync protects you

We're committed to protecting your security and privacy in the cloud



100% private cloud

End-to-end encryption protects your confidential data in the cloud from unauthorized access at all times. We can't read your files and no one else can either.



Your personal data belongs to you

Sync doesn't collect, sell or share your personal data or app usage information to advertisers or third-parties, and we do not claim ownership of your data.



Global data privacy compliance

Sync is safe to use, no matter where your business operates, with USA, EU / UK GDPR, and Canadian compliance built-in, including Canadian data residency.



Automatic backup, sync and restore

Sync backs up your files in realtime, and makes it easy to recover deleted files and previous versions of any file, any time. Never lose a file again.



Enterprise-grade infrastructure

Data is replicated across multiple SSAE 16 type 2 certified datacentre locations with SAS RAID storage, automatic failover and a 99.9% or better uptime SLA.



Account security controls

Two-factor authentication, granular user permissions, remote wipe, custom passwords, expiry dates, notifications and more ensure you're always in control.

Ease of use

If you're familiar with the cloud you'll be right at home with Sync, and if you're just getting started you'll be protecting your data in no time. Sync makes encryption easy, which means that your data is safe, secure and 100% private, simply by using Sync.

Get started

Create a free account (no credit card required) to try Sync out, for as long as you'd like. Upgrade anytime.

[Learn more about our plans and pricing](#)

[Create a free account right now](#)



Only you can access your files

Most cloud storage providers differ from Sync because they can access, scan and read your files. Sync's end-to-end encrypted storage platform and apps ensure that only you can access your data in the cloud. We can't read your files and no one else can either.

 [Read our privacy whitepaper](#)

 [Watch our video \(2 minutes\)](#)

Browse Privately. Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

[Download Tor Browser](#) ↓



BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies automatically clear when you're done browsing. So will your browsing history.

DEFEND AGAINST SURVEILLANCE

Tor Browser prevents someone watching your connection from knowing what websites you visit. All anyone monitoring your browsing habits can see is that you're using Tor.



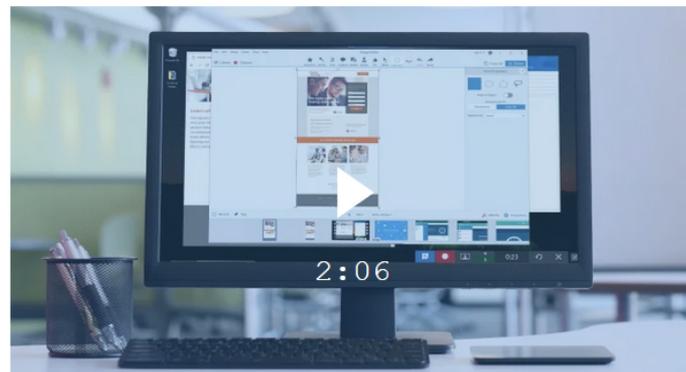
RESIST FINGERPRINTING

Tor Browser aims to make all users look the same, making it difficult for you to be fingerprinted based on your browser and device information.

Simple and Powerful

Screen Capture and Recording Software

Snagit lets you quickly capture a process, add your explanation, and create visual instructions.



Download Free Trial

★★★★★ 4.5 (1393)

Over 14 million people worldwide use Snagit



MAKE VISUAL
HOW-TO GUIDES



GIVE QUICK,
SIMPLE ANSWERS



PROVIDE BETTER
FEEDBACK



TRANSFORM
YOUR
COMMUNICATION



POSTAGE ON DEMAND[®]

Print your own postage and shipping labels in seconds.



CLICK

Instantly buy and calculate exact postage.



PRINT

Print postage on labels, envelopes or plain paper.



MAIL

Affix postage and mail anywhere in the world.

[GET STARTED](#)

CORPORATE POSTAGE SOLUTIONS

Have more than 2 locations? Then Stamps.com Enterprise is the postage solution for you. 

SHIPPING SOLUTIONS

Process and print shipping labels fast, enjoy shipping discounts and more. 

STAMPS.COM vs. POSTAGE METERS

The choice is clear. Stamps.com offers more features at a fraction of the cost. 

Give us a try!

Get

\$5

in **FREE**
Postage!*

*to use during your trial

[Offer Details](#)

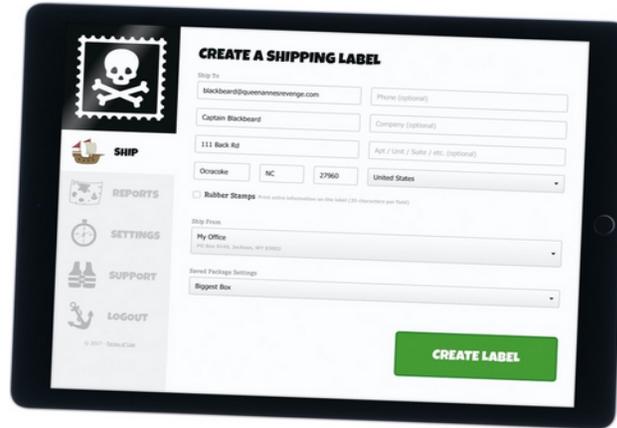




Rates Features Help

Login

Create a FREE account



Get the cheapest shipping rates for all USPS® services

Save up to 90% off retail USPS rates with the deepest commercial discounts and no markup, monthly fees, or hidden costs.

[Here's how it works](#)

Enter your email address

Create your FREE account



Features

Keep your team consistent, accurate, and current

Share your snippets with your team to keep them on track. Keep your whole sales team on message. Give your whole support team the current answers to all your customer questions.

- Integrated TextExpander online service and Apps
- Access your snippets on all your devices with your TextExpander user account
- Current snippets and edits everywhere
- Share snippets easily with coworkers and friends
- You pick who can edit your shared snippets
- Setup an Organization to easily manage and share snippets with your team
- Automatically join an organization using your company email address
- Automatically share company snippets with anyone who joins your organization

Work faster and smarter

Use TextExpander's powerful snippets and abbreviations to streamline and speed all you type. Create powerful snippets to save you time so that all you type is a short abbreviation, and TextExpander does the rest of the typing for you.

- Expand your snippets in any application from single lines to whole paragraphs
- Style your snippet text and add images and links.
- System-wide spelling correction in multiple languages
- Group snippets and print by group
- Search and expand snippets, abbreviations, and suggestions inline as you type
- Reminders to use your snippets and suggestions as you type

Customize the standardized

Streamline your email. Take boilerplate email responses or sales queries and customize just the areas that you need. You wear many hats, use your email signature du jour, with current social media links!

- Use fill-in-the-blank snippets to create custom forms with multiple field types and sections
- Expand a snippet as part of another by nesting
- Automatically insert clipboard content in a snippet
- Position the cursor wherever you want in your expanded snippet
- Create perfect email signatures, one for every occasion
- Create snippets and signatures with formatted text, pictures and links

**RULE 1.6:
CONFIDENTIALITY OF INFORMATION**

(a) **A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:**

- (1) **the client gives informed consent, as defined in Rule 1.0(j);**
- (2) **the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or**
- (3) **the disclosure is permitted by paragraph (b).**

“Confidential information” consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. “Confidential information” does not ordinarily include (i) a lawyer’s legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) **A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:**

- (1) **to prevent reasonably certain death or substantial bodily harm;**
- (2) **to prevent the client from committing a crime;**
- (3) **to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;**
- (4) **to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer’s firm or the law firm;**
- (5) **(i) to defend the lawyer or the lawyer’s employees and associates against an accusation of wrongful conduct; or**
 - (ii) **to establish or collect a fee; or**
- (6) **when permitted or required under these Rules or to comply with other law or court order.**

(c) A lawyer make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Comment

Scope of the Professional Duty of Confidentiality

[1] This Rule governs the disclosure of information protected by the professional duty of confidentiality. Such information is described in these Rules as “confidential information” as defined in this Rule. Other rules also deal with confidential information. See Rules 1.8(b) and 1.9(c)(1) for the lawyer’s duties with respect to the use of such information to the disadvantage of clients and former clients; Rule 1.9(c)(2) for the lawyer’s duty not to reveal information relating to the lawyer’s prior representation of a former client; Rule 1.14(c) for information relating to representation of a client with diminished capacity; Rule 1.18(b) for the lawyer’s duties with respect to information provided to the lawyer by a prospective client; Rule 3.3 for the lawyer’s duty of candor to a tribunal; and Rule 8.3(c) for information gained by a lawyer or judge while participating in an approved lawyer assistance program.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client’s informed consent, or except as permitted or required by these Rules, the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source. See Rule 1.0(j) for the definition of informed consent. The lawyer’s duty of confidentiality contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer, even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Typically, clients come to lawyers to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is thereby upheld.

[3] The principle of client-lawyer confidentiality is given effect in three related bodies of law: the attorney-client privilege of evidence law, the work-product doctrine of civil procedure and the professional duty of confidentiality established in legal ethics codes. The attorney-client privilege and the work-product doctrine apply when compulsory process by a judicial or other governmental body seeks to compel a lawyer to testify or produce information or evidence concerning a client. The professional duty of client-lawyer confidentiality, in contrast, applies to a lawyer in all settings and at all times, prohibiting the lawyer from disclosing confidential information unless permitted or required by these Rules or to comply with other law or court order. The confidentiality duty applies not only to matters communicated in confidence by the client, which are protected by the attorney-client privilege, but also to all information gained during and relating to the representation, whatever its source. The confidentiality duty, for example, prohibits a lawyer from volunteering confidential information to a friend or to any other person except in compliance with the provisions of this Rule, including the Rule’s reference to other law that may compel disclosure. See Comments [12]-[13]; see also Scope.

[4] Paragraph (a) prohibits a lawyer from knowingly revealing confidential information as defined by this Rule. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal confidential information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation with persons not connected to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client.

[4A] Paragraph (a) protects all factual information "gained during or relating to the representation of a client." Information relates to the representation if it has any possible relevance to the representation or is received because of the representation. The accumulation of legal knowledge or legal research that a lawyer acquires through practice ordinarily is not client information protected by this Rule. However, in some circumstances, including where the client and the lawyer have so agreed, a client may have a proprietary interest in a particular product of the lawyer's research. Information that is generally known in the local community or in the trade, field or profession to which the information relates is also not protected, unless the client and the lawyer have otherwise agreed. Information is not "generally known" simply because it is in the public domain or available in a public file.

Use of Information Related to Representation

[4B] The duty of confidentiality also prohibits a lawyer from using confidential information to the advantage of the lawyer or a third person or to the disadvantage of a client or former client unless the client or former client has given informed consent. See Rule 1.0(j) for the definition of "informed consent." This part of paragraph (a) applies when information is used to benefit either the lawyer or a third person, such as another client, a former client or a business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of land, the lawyer may not (absent the client's informed consent) use that information to buy a nearby parcel that is expected to appreciate in value due to the client's purchase, or to recommend that another client buy the nearby land, even if the lawyer does not reveal any confidential information. The duty also prohibits disadvantageous use of confidential information unless the client gives informed consent, except as permitted or required by these Rules. For example, a lawyer assisting a client in purchasing a parcel of land may not make a competing bid on the same land. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client, even to the disadvantage of the former client, after the client-lawyer relationship has terminated. *See* Rule 1.9(c)(1).

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer may make disclosures of confidential information that are impliedly authorized by a client if the disclosures (i) advance the best interests of the client and (ii) are either reasonable under the circumstances or customary in the professional community. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. In addition, lawyers in a firm may, in the course of the firm's practice, disclose to each other

information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers. Lawyers are also impliedly authorized to reveal information about a client with diminished capacity when necessary to take protective action to safeguard the client's interests. See Rules 1.14(b) and (c).

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions that prevent substantial harm to important interests, deter wrongdoing by clients, prevent violations of the law, and maintain the impartiality and integrity of judicial proceedings. Paragraph (b) permits, but does not require, a lawyer to disclose information relating to the representation to accomplish these specified purposes.

[6A] The lawyer's exercise of discretion conferred by paragraphs (b)(1) through (b)(3) requires consideration of a wide range of factors and should therefore be given great weight. In exercising such discretion under these paragraphs, the lawyer should consider such factors as: (i) the seriousness of the potential injury to others if the prospective harm or crime occurs, (ii) the likelihood that it will occur and its imminence, (iii) the apparent absence of any other feasible way to prevent the potential injury, (iv) the extent to which the client may be using the lawyer's services in bringing about the harm or crime, (v) the circumstances under which the lawyer acquired the information of the client's intent or prospective course of action, and (vi) any other aggravating or extenuating circumstances. In any case, disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to prevent the threatened harm or crime. When a lawyer learns that a client intends to pursue or is pursuing a course of conduct that would permit disclosure under paragraphs (b)(1), (b)(2) or (b)(3), the lawyer's initial duty, where practicable, is to remonstrate with the client. In the rare situation in which the client is reluctant to accept the lawyer's advice, the lawyer's threat of disclosure is a measure of last resort that may persuade the client. When the lawyer reasonably believes that the client will carry out the threatened harm or crime, the lawyer may disclose confidential information when permitted by paragraphs (b)(1), (b)(2) or (b)(3). A lawyer's permissible disclosure under paragraph (b) does not waive the client's attorney-client privilege; neither the lawyer nor the client may be forced to testify about communications protected by the privilege, unless a tribunal or body with authority to compel testimony makes a determination that the crime-fraud exception to the privilege, or some other exception, has been satisfied by a party to the proceeding. For a lawyer's duties when representing an organizational client engaged in wrongdoing, see Rule 1.13(b).

[6B] Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial risk that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to

eliminate the threat or reduce the number of victims. Wrongful execution of a person is a life-threatening and imminent harm under paragraph (b)(1) once the person has been convicted and sentenced to death. On the other hand, an event that will cause property damage but is unlikely to cause substantial bodily harm is not a present and substantial risk under paragraph (b)(1); similarly, a remote possibility or small statistical likelihood that any particular unit of a mass-distributed product will cause death or substantial bodily harm to unspecified persons over a period of years does not satisfy the element of reasonably certain death or substantial bodily harm under the exception to the duty of confidentiality in paragraph (b)(1).

[6C] Paragraph (b)(2) recognizes that society has important interests in preventing a client's crime. Disclosure of the client's intention is permitted to the extent reasonably necessary to prevent the crime. In exercising discretion under this paragraph, the lawyer should consider such factors as those stated in Comment [6A].

[6D] Some crimes, such as criminal fraud, may be ongoing in the sense that the client's past material false representations are still deceiving new victims. The law treats such crimes as continuing crimes in which new violations are constantly occurring. The lawyer whose services were involved in the criminal acts that constitute a continuing crime may reveal the client's refusal to bring an end to a continuing crime, even though that disclosure may also reveal the client's past wrongful acts, because refusal to end a continuing crime is equivalent to an intention to commit a new crime. Disclosure is not permitted under paragraph (b)(2), however, when a person who may have committed a crime employs a new lawyer for investigation or defense. Such a lawyer does not have discretion under paragraph (b)(2) to use or disclose the client's past acts that may have continuing criminal consequences. Disclosure is permitted, however, if the client uses the new lawyer's services to commit a further crime, such as obstruction of justice or perjury.

[6E] Paragraph (b)(3) permits a lawyer to withdraw a legal opinion or to disaffirm a prior representation made to third parties when the lawyer reasonably believes that third persons are still relying on the lawyer's work and the work was based on "materially inaccurate information or is being used to further a crime or fraud." *See* Rule 1.16(b)(1), requiring the lawyer to withdraw when the lawyer knows or reasonably should know that the representation will result in a violation of law. Paragraph (b)(3) permits the lawyer to give only the limited notice that is implicit in withdrawing an opinion or representation, which may have the collateral effect of inferentially revealing confidential information. The lawyer's withdrawal of the tainted opinion or representation allows the lawyer to prevent further harm to third persons and to protect the lawyer's own interest when the client has abused the professional relationship, but paragraph (b)(3) does not permit explicit disclosure of the client's past acts unless such disclosure is permitted under paragraph (b)(2).

[7] [Reserved.]

[8] [Reserved.]

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about compliance with these Rules and other law by the lawyer, another lawyer in the lawyer's firm, or the law firm. In many situations, disclosing information to secure

such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with these Rules, court orders and other law.

[10] Where a claim or charge alleges misconduct of the lawyer related to the representation of a current or former client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. Such a claim can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, such as a person claiming to have been defrauded by the lawyer and client acting together or by the lawyer acting alone. The lawyer may respond directly to the person who has made an accusation that permits disclosure, provided that the lawyer's response complies with Rule 4.2 and Rule 4.3, and other Rules or applicable law. A lawyer may make the disclosures authorized by paragraph (b)(5) through counsel. The right to respond also applies to accusations of wrongful conduct concerning the lawyer's law firm, employees or associates.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Paragraph (b) does not mandate any disclosures. However, other law may require that a lawyer disclose confidential information. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of confidential information appears to be required by other law, the lawyer must consult with the client to the extent required by Rule 1.4 before making the disclosure, unless such consultation would be prohibited by other law. If the lawyer concludes that other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

[13] A tribunal or governmental entity claiming authority pursuant to other law to compel disclosure may order a lawyer to reveal confidential information. Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason. In the event of an adverse ruling, the lawyer must consult with the client to the extent required by Rule 1.4 about the possibility of an appeal or further challenge, unless such consultation would be prohibited by other law. If such review is not sought or is unsuccessful, paragraph (b)(6) permits the lawyer to comply with the order.

[14] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified in paragraphs (b)(1) through (b)(6). Before making a disclosure, the lawyer should, where practicable, first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose, particularly when accusations of wrongdoing in the representation of a client have been made by a third party rather than by the client. If the disclosure will be made in connection with an adjudicative proceeding, the disclosure should be

made in a manner that limits access to the information to the tribunal or other persons having a need to know the information, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[15] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may, however, be required by other Rules or by other law. *See* Comments [12]-[13]. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). *E.g.*, Rule 8.3(c)(1). Rule 3.3(c), on the other hand, requires disclosure in some circumstances whether or not disclosure is permitted or prohibited by this Rule.

Withdrawal

[15A] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw pursuant to Rule 1.16(b)(1). Withdrawal may also be required or permitted for other reasons under Rule 1.16. After withdrawal, the lawyer is required to refrain from disclosing or using information protected by Rule 1.6, except as this Rule permits such disclosure. Neither this Rule, nor Rule 1.9(c), nor Rule 1.16(e) prevents the lawyer from giving notice of the fact of withdrawal. For withdrawal or disaffirmance of an opinion or representation, see paragraph (b)(3) and Comment [6E]. Where the client is an organization, the lawyer may be in doubt whether the organization will actually carry out the contemplated conduct. Where necessary to guide conduct in connection with this Rule, the lawyer may, and sometimes must, make inquiry within the organization. *See* Rules 1.13(b) and (c).

Duty to Preserve Confidentiality

[16] Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are otherwise subject to the lawyer's supervision. *See* Rules 1.1, 5.1 and 5.3. Confidential information includes not only information protected by Rule 1.6(a) with respect to current clients but also information protected by Rule 1.9(c) with respect to former clients and information protected by Rule 1.18(b) with respect to prospective clients. Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by Rules 1.6, 1.9, or 1.18, does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule, or may give informed consent to forgo security measures that would otherwise be required by this Rule. For a lawyer's duties when sharing information with nonlawyers inside or outside the lawyer's own firm, see Rule 5.3, Comment [2].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of confidentiality. However, a lawyer may be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information). For example, a protective order may extend a high level of protection to documents marked "Confidential" or "Confidential – Attorneys' Eyes Only"; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") may require a lawyer to take specific precautions with respect to a client's or adversary's medical records; and court rules may require a lawyer to block out a client's Social Security number or a minor's name when electronically filing papers with the court. The specific requirements of court orders, court rules, and other laws are beyond the scope of these Rules.

Lateral Moves, Law Firm Mergers, and Confidentiality

[18A] When lawyers or law firms (including in-house legal departments) contemplate a new association with other lawyers or law firms through lateral hiring or merger, disclosure of limited information may be necessary to resolve conflicts of interest pursuant to Rule 1.10 and to address financial, staffing, operational, and other practical issues. However, Rule 1.6(a) requires lawyers and law firms to protect their clients' confidential information, so lawyers and law firms may not disclose such information for their own advantage or for the advantage of third parties absent a client's informed consent or some other exception to Rule 1.6.

[18B] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter, including the general issues involved; (iii) information that is publicly available; (iv) the lawyer's total book of business; (v) the financial terms of each lawyer-client relationship; and (vi) information about aggregate current and historical payment of fees (such as realization rates, average receivables, and aggregate timeliness of payments). Such information is generally not "confidential information" within the meaning of Rule 1.6.

[18C] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily *not* permitted, however, if information is protected by Rule 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney-client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness in paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; or information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client's conduct).

[18D] When lawyers are exploring a new association, whether by lateral move or by merger, all lawyers involved must individually consider fiduciary obligations to their existing firms that may bear on the timing and scope of disclosures to clients relating to conflicts and financial concerns, and should consider whether to ask clients for a waiver of confidentiality if consistent with these fiduciary duties – *see* Rule 1.10(e) (requiring law firms to check for conflicts of interest). Questions of fiduciary duty are legal issues beyond the scope of the Rules.

[18E] For the unique confidentiality and notice provisions that apply to a lawyer or law firm seeking to sell all or part of its practice, see Rule 1.17 and Comment [7] to that Rule.

[18F] Before disclosing information regarding a possible lateral move or law firm merger, law firms and lawyers moving between firms – both those providing information and those receiving information – should use reasonable measures to minimize the risk of any improper, unauthorized or inadvertent disclosures, whether or not the information is protected by Rule 1.6(a), 1.9(c), or 1.18(b). These steps might include such measures as: (1) disclosing client information in stages; initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information outside the firm(s) during and after the lateral hiring negotiations or merger process.

Purchased 3 times.

You purchased this item on November 30, 2019.

Style: B01N49R9KP | [View this order](#)



Brother QL-800 High-Speed Professional Label Printer, Lightning Quick Printing, Plug & Label Feature, Brother Genuine DK Pre-Sized Labels, Multi-System Compatible – Black & Red Printing Available

by [Brother](#)

★★★★☆ [385 ratings](#)

| [253 answered questions](#)

Amazon's Choice for "brother l..."

List Price: ~~\$99.99~~

Price: **\$58.99**

\$58.99

prime FREE One-Day

FREE delivery: **Tomorrow**

Order within 3 hrs 2 mins [Details](#)

[Bill - Hamilton 13346](#)

In Stock.

Qty: 1



Add to Cart



Buy Now

Ships from and sold by Amazon.com.

Add a Protection Plan:

[4-Year Protection](#) for **\$9.99**

P-touch PT-P900 Series: On-Demand Label Solutions

Create tough, laminated labels built to last with the P-touch PT-P900 Series desktop and barcode label printers.

[Explore Features ↓](#)

[Compare Models ↓](#)

[Try One for Free ↓](#)

