Computer Security

Scammers, hackers and identity thieves are looking to steal your personal information - and your money. But there are steps you can take to protect yourself, like keeping your computer software up-to-date and giving out your personal information only when you have good reason.

Update Your Software. Keep your software – including your operating system, the web browsers you use to connect to the Internet, and your apps – up to date to protect against the latest threats. Most software can update automatically, so make sure to set yours to do so.
Outdated software is easier for criminals to break into. If you think you have a virus or bad software on your computer, check out how to detect and get rid of malware.

Protect Your Personal Information. Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about why someone needs it and whether you can really trust the request.
In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Protect Your Passwords. Here are a few ideas for creating strong passwords and keeping them safe:

- Use at least 10 characters; 12 is ideal for most home users.

- Try to be unpredictable – don't use names, dates, or common words. Mix numbers, symbols, and capital letters into the middle of your password, not at the beginning or end.
- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies where you do business – thieves can use it to take over all your accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not ask you for your password.
- If you write down a password, keep it locked up, out of plain sight.

Consider Turning On Two-Factor Authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

Give Personal Information Over Encrypted Websites Only. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address. That means the site is secure.

Back Up Your Files. No system is completely secure. Copy your files to an external hard drive or cloud storage. If your computer is attacked by malware, you'll still have access to your files.

Malware

Malware includes viruses, spyware, and other unwanted software that gets installed on your computer or mobile device without your consent. These programs can cause your device to crash, and can be used to monitor and control your online activity. They also can make your computer vulnerable to viruses and deliver unwanted or inappropriate ads. Criminals use malware to steal personal information, send spam, and commit fraud.

- **Avoid Malware**

Avoid Malware

Scam artists try to trick people into clicking on links that will download viruses, spyware, and other unwanted software — often by bundling it with popular free downloads. To reduce your risk of downloading malware:

- **Install and update security software, and use a firewall.** Set your security software, internet browser, and operating system (like Windows or Mac OS X) to update automatically.
- **Don't change your browser's security settings.** You can minimize "drive-by" or bundled downloads if you keep your browser's default security settings.
- **Pay attention to your browser's security warnings.** Many browsers come with built-in security scanners that warn you before you visit an infected webpage or download a malicious file.
- **Instead of clicking on a link in an email, type the URL of a trusted site directly into your browser.** Criminals send emails that appear to be from companies you know and trust. The links may look legitimate, but clicking on them could download malware or send you to a scam site.
- **Don't open attachments in emails unless you know who sent it and what it is.** Opening the wrong attachment — even if it seems to be from friends or family — can install malware on your computer.
- **Get well-known software directly from the source.** Sites that offer lots of different browsers, PDF readers, and other popular software for free are more likely to include malware.
- **Read each screen when installing new software**. If you don't recognize a program, or are prompted to install additional "bundled" software, decline the additional program or exit the installation process.
- **Don't click on popups or banner ads about your computer's performance.** Scammers insert unwanted software into banner ads that look legitimate, especially ads about your computer's health. Avoid clicking on these ads if you don't know the source.
- **Scan USBs and other external devices before using them.** These devices can be infected with malware, especially if you

use them in high traffic places, like photo printing stations or public computers.
- **Talk about safe computing.** Tell your friends and family that some online actions can put the computer at risk: clicking on pop-ups, downloading "free" games or programs, opening chain emails, or posting personal information.
- **Back up your data regularly**. Whether it's your taxes, photos, or other documents that are important to you, back up any data that you'd want to keep in case your computer crashes.

Detect Malware

Monitor your computer for unusual behavior. Your computer may be infected with malware if it:

- slows down, crashes, or displays repeated error messages
- won't shut down or restart
- serves a barrage of pop-ups
- serves inappropriate ads or ads that interfere with page content
- won’t let you remove unwanted software
- injects ads in places you typically wouldn’t see them, such as government websites
- displays web pages you didn't intend to visit, or sends emails you didn't write

Other warning signs of malware include:

- new and unexpected toolbars or icons in your browser or on your desktop
- unexpected changes in your browser, like using a new default search engine or displaying new tabs you didn’t open
- a sudden or repeated change in your computer's internet home page
- a laptop battery that drains more quickly than it should

Get Rid of Malware

If you suspect there is malware on your computer, take these steps:

- **Stop shopping, banking, and doing other online activities** that involve user names, passwords, or other sensitive information.

- **Update your security software**, and then scan your computer for viruses and spyware. Delete anything it identifies as a problem. You may have to restart your computer for the changes to take effect.
- **Check your browser** to see if it has tools to delete malware or reset the browser to its original settings.
- **If your computer is covered by a warranty** that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem.
- **Many companies — including some affiliated with retail stores — offer tech support.** Telephone and online help usually are less expensive, but online search results might not be the best way to find help. Tech support scammers pay to boost their ranking in search results so their websites and phone numbers appear above those of legitimate companies. If you want tech support, look for a company's contact information on their software package or on your receipt.

Securing Your Wireless Network

Today's home network may include a wide range of wireless devices, from computers and phones, to IP Cameras, smart TVs and connected appliances. Taking basic steps to secure your home network will help protect your devices – and your information – from compromise.

Understand How a Wireless Network Works

Going wireless generally requires connecting an internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any device within range can pull the signal from the air and access the internet.

Unless you take certain precautions, anyone nearby can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network or access information on your device. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

Use Encryption on Your Wireless Network

Once you go wireless, you should encrypt the information you send over your wireless network, so that nearby attackers can't eavesdrop on these communications. Encryption scrambles the information you send into a code so that it's not accessible to others. Using encryption is the most effective way to secure your network from intruders.

Two main types of encryption are available for this purpose: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption.

WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Some older routers use only WEP encryption, which likely won't protect you from some common hacking programs. Consider buying a new router with WPA2 capability.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website.

Limit Access to Your Network

Allow only specific devices to access your wireless network. Every device that is able to communicate with a network is assigned a unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

Secure Your Router

It's also important to protect your network from attacks over the internet by keeping your router secure. Your router directs traffic between your local network and the internet. So, it's your first line of defense for guarding against such attacks. If you don't take steps to secure your router, strangers could gain access to sensitive personal or financial information on your device. Strangers also could seize control of your router, to direct you to fraudulent websites.

Change the name of your router from the default. The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.

Change your router's pre-set password(s). The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router, as its "administrator." Hackers know these default passwords, so change it to something only you know. The same goes for any default "user" passwords. Use long and complex passwords – think at least 12 characters, with a mix of numbers, symbols, and upper and lower case letters. Visit the company's website to learn how to change the password.

Turn off any "Remote Management" features. Some routers offer an option to allow remote access to your router's controls, such as to enable the manufacturer to provide technical support. Never leave this feature enabled. Hackers can use them to get into your home network.
Log out as Administrator: Once you've set up your router, log out as administrator, to lessen the risk that someone can piggyback on your session to gain control of your device.
Keep your router up-to-date: To be secure and effective, the software that comes with your router needs occasional updates. Before you set up a new router and periodically thereafter, visit the manufacturer's website to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates.
And when you secure your router, don't forget to secure your computer too. Use the same basic computer security practices that you would for any computer connected to the internet. For example, use protections like antivirus, antispyware, and a firewall -- and keep these protections up-to-date.

Protect Your Network during Mobile Access

Apps now allow you to access your home network from a mobile device. Before you do, be sure that some security features are in place.

Use a strong password on any app that accesses your network. Log out of the app when you're not using it. That way, no one else can access the app if your phone is lost or stolen.
Password protect your phone or other mobile device. Even if your app has a strong password, it's best to protect your device with one, too.

\

Tips for Using Public Wi-Fi Networks

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they're not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, it might be accessed by someone else.

To protect your information when using wireless hotspots, send information only to sites that are fully encrypted, and avoid using mobile apps that require personal or financial information.

How Encryption Works

Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code so it's not accessible to others. When you're using wireless networks, it's best to send personal information only if it's encrypted — either by an encrypted website or a secure Wi-Fi network. An encrypted website protects **only** the information you send **to and from that site**. A secure wireless network encrypts **all** the information you send using that network.

How to Tell If a Website is Encrypted

If you send email, share digital photos and videos, use social networks, or bank online, you're sending personal information over the internet. The information you share is stored on a server — a powerful computer that collects and delivers content. Many websites, like banking sites, use encryption to protect your information as it travels from your computer to their server.

To determine if a website is encrypted, look for **https** at the start of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for **https** on **every** page you visit, not just when you sign in.

What About Mobile Apps?

Unlike websites, mobile apps don't have a visible indicator like **https**. Researchers have found that many mobile apps don't encrypt information

properly, so it's a bad idea to use certain types of mobile apps on unsecured Wi-Fi. If you plan to use a mobile app to conduct sensitive transactions — like filing your taxes, shopping with a credit card, or accessing your bank account — use a secure wireless network or your phone's data network (often referred to as 3G or 4G).
If you must use an unsecured wireless network for transactions, use the company's mobile website — where you can check for the **https** at the start of the web address — rather than the company's mobile app.

Don't Assume a Wi-Fi Hotspot is Secure

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and **aren't** secure. In fact, if a network doesn't require a WPA or WPA2 password, it's probably not secure.
If you use an unsecured network to log in to an unencrypted site — or a site that uses encryption only on the sign-in page — other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools — available for free online — make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people in your contact lists. In addition, a hacker could test your username and password to try to gain access to other websites – including sites that store your financial information.

Protect Your Information When Using Public Wi-Fi

Here's how you can protect your information when using Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.

- Do not use the same password on different websites. It could give someone who gains access to **one**of your accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees. What's more, VPN options are available for mobile devices; they can encrypt information you send through mobile apps.
- Some Wi-Fi networks use encryption: WEP and WPA are common, but they might not protect you against all hacking programs. WPA2 is the strongest.
- Installing browser add-ons or plug-ins can help. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites — look for **https** in the URL to know a site is secure.
- Take steps to secure your home wireless network.

Virtual Private Network (VPN) apps

You probably know by now that using your mobile device on the public Wi-Fi network of your local coffee shop or airport poses some risk. Public networks are not very secure – or, well, private – which makes it easy for others to intercept your data. So, what can you do to keep your mobile data private and secure while out and about? Some consumers have started using Virtual Private Network (VPN) apps to shield the information on their mobile devices from prying eyes on public networks. Before you download a VPN app, you should know that there are benefits and risks.

VPN app basics

How do VPN apps work? When you use a VPN app, data sent from your phone – be it your browsing data or the apps you are using – is routed through servers located elsewhere. A VPN app can make traffic from your phone to a website you visit appear to come from a server operated by the VPN provider, rather than directly from your phone. Some VPN apps also encrypt the data sent between your phone and the VPN server. So, for example, say you are using a public Wi-Fi network that isn't secure – such as a network that allows anyone to use it, even if they don't have a password. Other people on the same network can see your traffic. But when you use a VPN app that encrypts the data, anyone monitoring your network connection only sees gibberish – even if the particular site you are visiting doesn't itself employ encryption.

Why would someone use a VPN app? VPN apps tout a variety of uses. Not only do some VPN apps promise to keep your information secure on public networks, but some also claim they will keep your information private from advertisers and other third parties. And because VPN apps route your traffic through another network, they can make it appear as if your traffic is coming from somewhere else. This is similar to how a company might use a VPN to allow employees to use their work computer as if they were on the company's network, even while they're on the road.

What are some privacy and data security concerns about using a VPN app? First, you should be aware that when you use a VPN app, you are giving the app permission to intercept all of your internet traffic. You don't want to grant such permission lightly. Also, a group of technical researchers who studied almost 300 VPN apps found (link is external) potential privacy and security risks with some VPN apps. According to the study, for example, some VPN apps did not use encryption; some requested sensitive, and possibly unexpected, privileges; and some shared data with third parties for purposes such as injecting or serving ads, or analyzing the data to see how people are using a particular site or service. Given these findings and the considerable trust you must place in a VPN app with your traffic, here are some things to consider before you download a VPN app.

Before you download a VPN app

- **Research the VPN app before you use it.** You are trusting a VPN with potentially all of your traffic. Before you download a VPN app, learn as much about the app as you can. Look up outside reviews from sources you respect. You can also look at screenshots, the app's description, its content rating, and user reviews, and can do some online research on the developer. The fact that an app promises security or privacy does not necessarily make it trustworthy.
- **Carefully review the permissions the app requests.** Apps will present the permissions they request on their app store page, during installation, or at the time they use the permission. It's useful information that tells you what types of information the app will access on your device in addition to your internet traffic. If an app requests particularly sensitive permissions (reading text messages, for example), consider whether the permission makes sense given the app's purpose and whether you trust the app developer with that access.
- **Know that not all VPN apps actually encrypt your information.** Some VPN apps use protocols that do not encrypt your traffic, or encrypt only some of your traffic. Outside reviews from sources you respect might provide more information about a particular app's use of encryption.
- **A VPN app generally isn't going to make you entirely anonymous.** Instead, the app will typically obscure the content of your traffic from your internet service provider or public Wi-Fi provider, shifting trust from those networks to the VPN app provider.

In addition, sites you visit may be able to determine that you are using a VPN app, and can still use any identifying information you directly share with them (for example, filling out a form with your email address) to track you.

- **VPN apps may share your information with third parties.** Many VPN apps are free because they sell advertising within the app, or because they share your information with (or redirect your traffic through) third parties. If you are using the VPN app to keep your traffic private, make sure you review the VPN app's terms and conditions and its privacy policy to determine if it shares information with third parties such as advertisers, and if so, what information it shares.

Apps to Help You Shop in Stores

A *good* shopping buddy has a sharp eye, knows the lay of the land, and can find the best deals on the products you want. A *great* shopping buddy might even share coupons with you. Millions of people have found new shopping buddies – their smartphones. "Shopping apps" for use in brick-and-mortar stores have been downloaded millions of times.

What Can Shopping Apps Do?

Apps to help you shop in physical stores may have several types of features:

In-store purchases

These apps allow you to pay on-site, using your phone for checkout. Many use a bar code or quick response (QR) code scanner. When it's time to pay, instead of swiping a card or using cash, you open the app so the store clerk can scan the bar or QR code on your phone. Some apps let you pay by tapping your phone against an electronic reader.

To fund in-store purchases, you link the app to your credit card, debit card, gift card or prepaid card. Some apps are called "pass through" – they charge your card or bank account each time you buy something.

Others let you store value with the app and spend from the stored value every time you buy something.

Price comparison

These apps help you check for the best available price in real time. Many of these apps use your phone's camera to scan a product code.

Then they search online databases to show you prices and information about similar products sold online or in stores.

Deals

These apps help you find, earn or redeem coupons or loyalty points when you shop in-store. Some apps offer specific discounts based on information they collect from your phone, like your location or purchase history.

Many shopping apps combine these features. For example, some retailers have in-store purchase apps for use only in their stores; the same apps also offer coupons for their products.

What if I Discover a Billing Error or Unauthorized Charge When I Use an In-store Purchase App?

If you have a billing problem after using a shopping app in a store, turn to the store, the app or the credit or debit card linked to the app for help.

The store

You can solve many payment issues by talking to a store employee. Do this as soon as possible because some retailers have time limits on returns and refunds. If you used an app developed by the retailer, it's likely their employees would help you work out any problems.

If the first employee doesn't have the authority to help you, ask for a supervisor or manager. With each person, explain the problem and ask what they will do to fix it. Keep a record of your conversations — who you spoke to and when, and what they promised to do.

The app

According to an FTC staff study, user agreements for shopping apps generally offer few promises that the app company will help if you have a problem. In fact, some user agreements claim the company doesn't have to take responsibility for any problems. The company may behave better than that, but there are no guarantees.

Before you use a shopping app, look for:

- contact information
- how quickly you have to report unauthorized charges
- any limits on your responsibility for unauthorized charges
- if the company will investigate your claim, and how quickly the company will share the results of its investigation.

The app's help section, frequently asked questions or terms of use may have this information.

The credit or debit card

If the in-store purchase app is a "pass through," charging your credit or debit card each time you buy something, the legal protections for your credit or debit card apply:

Liability for Unauthorized Charges Varies by Payment Method

Payment Method	By law, your responsibility for unauthorized charges is limited to:
Credit Card	$50
Debit Card	$50 if you report within 2 business days after discovery $500 if you report after 2 business days, but within 60 days after your statement is sent to you that first shows the problem All charges if you don't report it within 60 days after your statement is sent to you that first shows the problem
Gift Cards, Virtual Currency, or Money Stored in an App	Generally, there is no legal limit on your liability. You're responsible for all charges, unless otherwise stated under the terms of service of your gift card.

If you use an app that requires you to store value with an up-front payment, you may not have the same protections as if you used a credit or debit card to make the same purchase directly. If you're considering a stored value app, see if it explains, upfront in the app description or user agreement, how the payment system works, and what to do if there's a

problem. If you can't find that information, use a different app, or keep the stored value to an amount you can afford to lose.

What Personal Information Do Shopping Apps Collect?

Shopping apps can collect a lot of information, like your name, mailing address, phone number and email. Many of these apps rely on location data to function. For example, some "deal" apps collect information about your location so they can send discounts automatically using text messages or push notifications when you're near a relevant business.

Some shopping apps say they might collect additional personal information, like your Social Security number, driver's license number, date of birth and gender. If you're asked for information like that, consider whether the convenience of the app is worth the risks that sensitive information is stored or shared by the app developer.

Shopping apps also may collect information about the things you buy, including how much you paid, when, where and how you paid. This information, combined with other personal data companies collect, may allow them to develop a detailed profile of you. Many of the privacy policies for mobile apps studied by the FTC allowed the app company to share users' data with other companies, like advertisers, data brokers or credit reporting companies.

Look for apps that tell you what they do with your data, and how they keep it secure. Many shopping apps offer strong promises about how they protect your personal information, and their privacy and security practices have to live up to their promises. If you think an app doesn't live up to its privacy or security promises, report it to the FTC.

Hacked Email

You get a flood of messages from friends and family. They're getting emails from you with seemingly random links, or messages with urgent pleas to wire you money. It looks like your email or social media account might have been taken over. What do you do? For starters, make sure your security protections are up-to-date, reset your password, and warn your friends.

How You Know You've Been Hacked

You might have been hacked if:

- friends and family are getting emails or messages you didn't send
- your Sent messages folder has messages you didn't send, or it has been emptied
- your social media accounts have posts you didn't make
- you can't log into your email or social media account

In the case of emails with random links, it's possible your email address was "spoofed," or faked, and hackers don't actually have access to your account. But you'll want to take action, just in case.

What To Do When You've Been Hacked

1. Update your system and delete any malware

Make sure your security software is up-to-date

If you don't have security software, get it. But install security software only from reputable, well-known companies. Then, run it to scan your computer for viruses and spyware (aka malware). Delete any suspicious software and restart your computer.

Set your security software, internet browser, and operating system (like Windows or Mac OS) to update automatically

Software developers often release updates to patch security vulnerabilities. Keep your security software, your internet browser, and your operating system up-to-date to help your computer keep pace with the latest hack attacks.

2. Change your passwords

That's IF you're able to log into your email or social networking account. Someone may have gotten your old password and changed it. If you use similar passwords for other accounts, change them, too. Make sure you create strong passwords that will be hard to guess.

3. Check the advice your email provider or social networking site has about restoring your account

You can find helpful advice specific to the service. If your account has been taken over, you might need to fill out forms to prove it's really you trying to get back into your account.

4. Check your account settings

Once you're back in your account, make sure your signature and "away" message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service, look for changes to the account since you last logged in — say, a new "friend."

5. Tell your friends

A quick email letting your friends know they might have gotten a malicious link or a fake plea for help can keep them from sending money they won't get back or installing malware on their computers. Put your friends' email addresses in the Bcc line to keep them confidential. You could copy and send this article, too.

What to Do Before You're Hacked

Use unique passwords for important sites, like your bank and email

That way, someone who knows one of your passwords won't suddenly have access to all your important accounts. Choose strong passwords that are harder to crack. Some people find password managers — software that stores and remembers your passwords for you — a helpful way to keep things straight. If you use a password manager, make sure to select a

unique, strong password for it, too. Many password managers will let you know whether the master password you've created is strong enough.

Safeguard your usernames and passwords

Think twice when you're asked to enter credentials like usernames and passwords. Never provide them in response to an email. If the email or text seems to be from your bank, for example, visit the bank website directly rather than clicking on any links or calling any numbers in the message. Scammers impersonate well-known businesses to trick people into giving out personal information.

Turn on two-factor authentication if your service provider offers it

A number of online services offer "two-factor authentication," where getting into your account requires a password plus something else — say, a code sent to your smartphone — to prove it's really you.

Don't click on links or open attachments in emails unless you know who sent them and what they are

That link or attachment could install malware on your computer. Also do your part: don't forward random links.

Download free software only from sites you know and trust

If you're not sure who to trust, do some research before you download any software. Free games, file-sharing programs, and customized toolbars also could contain malware.

Don't treat public computers like your personal computer

If it's not your computer, don't let a web browser remember your passwords, and make sure to log out of any accounts when you're done. In fact, if you can help it, don't access personal accounts — like email, or especially bank accounts — on public computers at all. (Also be careful any time you use public Wi-Fi.)

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day—and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $30 million to phishing schemes in one year. But there are several things you can do to protect yourself.

How to Recognize Phishing

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff

Here's a real world example of a phishing email.

Imagine you saw this in your inbox. **Do you see any signs that it's a scam?** Let's take a look.

- The email looks like it's from a company you may know and trust: Netflix. It even uses a Netflix logo and header.
- The email says your account is on hold because of a billing problem.
- The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email invites you to click on a link to update your payment details.

While, at a glance, this email might look real, it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can harm the reputation of the companies they're spoofing.

How to Protect Yourself From Phishing Attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it's a good idea to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

Four Steps to Protect Yourself From Phishing

1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.
2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.
3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

- Something you have—like a passcode you get via text message or an authentication app.
- Something you are—like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What to Do If You Suspect a Phishing Attack

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I have an account with the company or know the person that contacted me?**
If the answer is "No," it could be a phishing scam. Go back and review the tips in How to recognize phishing and look for signs of a phishing scam. If you see them, report the message and then delete it.
If the answer is "Yes," contact the company using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.

What to Do If You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost.
If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan.

How to Report Phishing

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you got a phishing email, forward it to the FTC at spam@uce.gov and to the Anti-Phishing Working Group at reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726).
Step 2. Report the phishing attack to the FTC at ftc.gov/complaint.
Tagged with: cyber security, phishing, scam

How to Spot, Avoid and Report Tech Support Scams

Share this page

- Facebook
- Twitter
- Linked-In

Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services you don't need, to fix a problem that doesn't exist. They often ask you to pay by wiring money, putting money on a gift card, prepaid card or cash reload card, or using a money transfer app because they know those types of payments can be hard to reverse.

- **Spotting and Avoiding Tech Support Scams**

- **What to Do If You Think There's a Problem With Your Computer**
- **What to Do If You Were Scammed**
- **Reporting Tech Support Scams**

Spotting and Avoiding Tech Support Scams

Tech support scammers use many different tactics to trick people. Spotting these tactics will help you avoid falling for the scam.

Phone Calls

Tech support scammers may call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist. Listen to an FTC undercover call with a tech support scammer.

If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up.

Pop-up Warnings

Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.

If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.

Online Ads and Listings in Search Results Pages

Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online. The scammers are hoping you'll call the phone number to get help.

If you're looking for tech support, go to a company you know and trust.

2 Things to Know to Avoid a Tech Support Scam

1. Legitimate tech companies won't contact you by phone, email or text message to tell you there's a problem with your computer.

2. Security pop-up warnings from real tech companies will never ask you to call a phone number.

What to Do If You Think There's a Problem With Your Computer

If you think there may be a problem with your computer, update your computer's security software and run a scan.
If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

What to Do If You Were Scammed

If you paid a tech support scammer with a credit or debit card, you may be able to stop the transaction. Contact your credit card company or bank right away. Tell them what happened and ask if they can reverse the charges.

If you paid a tech support scammer with a gift card, contact the company that issued the card right away. Tell them you paid a scammer with the gift card and ask if they can refund your money.
If you gave a scammer remote access to your computer, update your computer's security software. Then run a scan and delete anything it identifies as a problem.
If you gave your user name and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.

Avoid Tech Support Refund Scams
If someone calls to offer you a refund for tech support services you paid for, it's likely a fake refund scam. How does the scam work? The caller will ask if you were happy with the services you got. If you say, "No," they'll offer you a refund. In another variation, the caller says the company is giving out refunds because it's going out of business. No matter their story, they're not giving refunds. They're trying to steal more of your money. Don't give them your bank account, credit card or other payment information.

Reporting Tech Support Scams

If a tech support scammer contacts you, report it to the Federal Trade Commission. When you report a scam, the FTC can use the information to build cases against scammers. Are you skeptical that reporting scams will make a difference? Watch this video to learn how your story could help the FTC stop scammers.

Tech support scams are common. In 2017, the FTC received more than 150,000 reports about these scamsfrom people like you. Add your voice. Report tech support scams to the FTC.

Now that you know how to recognize a tech support scam, share what you learned with someone you know. You might help them avoid a tech support scam.

Tagged with: computer security, cyber security, online security, scam

How to improve your online security and privacy in 10 easy steps

Follow these ten easy steps to improve your online security and privacy quickly. The first five steps will help you to strengthen your online accounts. The other five will focus on hardening your computer.

Part I: Bulletproof your online accounts

1. Install a password manager: The golden rule for being safe online is to have a different random password for each site. Long and random passwords prevents brute-force attacks. Using a different password for each account prevents having all your accounts compromised at once when a data breach occurs because of password reuse. No one can generate and remember a gazillion random passwords, so the best way to do this is to use a password manager and just remember one very hard to guess password. My personal choice is LastPass but there are other good alternatives. **2. Update your accounts information**: Take a moment to go through your most important accounts and check they have the correct information, including email address and phone number. If

your password is weak, also take the time to upgrade it using your shiny new password manager. As shown in our recent research on secret questions, providing the correct phone number or email address greatly improves someones chances of recovering their account successfully.

3. Use two-factor authentication for important accounts: Add a second factor to the accounts for the services that you care the most about, such as Gmail, Dropbox, Facebook, Twitter, GitHub, iCloud and Steam. You can backup/sync your second factors for most sites using a third-party app such as authenticator plus (my favorite) or authy. In any case, dont forget to print the backup codes provided to you when you enable the second factor. You can also store them in your password manager.

4. Review your privacy settings: Review the settings on social networks and sharing sites to make sure your are sharing your data with whom you intend to. Facebook privacy setting step by step,Google+

5. Use a hardware security key for vital accounts: For the accounts that matter the most, it is worth going the extra mile and using a hardware security key as a second factor. Consider doing this for your main email account, your password manager and your recovery email address. For example, Google/Gmail uses FIDO U2F keys and LastPass uses the older Yubikeystandard, but you can get the two to work with one keyusing a Yubikey Neo.

Part II: Lock your computer down

6. Backup your valuable data: Backup the data you care about, photos, videos, documents, either on an external hard drive or in the cloud (or both!). This will save you from hardware failure, unwanted deletion and even cryptolocker malware. Use an external hard drive like the Seagate backup plus(recommended by Wirecutter) and/or back up your data in the cloud, for example, using Google Drive or Dropbox.

7. Update your operating system: Keeping your computer up to date is the first step to being safe online. Start by updating your operating system and turn on automatic updates if you havent done so. Windows, OSX and Linux support this. Consider also updating to the latest version of your operating system if you havent done so yet.

8. Keep your software up to date: Make sure your software, in particular your browser, is up to date to ensure you are safe while browsing the internet. Here is how to do this for Chrome, Firefox and Internet Explorer. Make sure the auto-update option of your various pieces of software is turned on.

9. Secure your computer: Make sure your antivirus and firewall are working properly. Here is how to check if your setup if correct forWindows 10 and OSX. Toms guide and other sites have review to help you choose the antivirus that fit you the best.

10. Respect browsers security warnings: Paying attentions to warming is probably the most obvious and still one of the most overlooked advice. Every modern browsers will show you a warning when you are about to visit a dangerous website. When you see one, as illustrated above, dont ignore them. Come back another time when the site is

cleaned up. Similarly dont download a program if your browser or antivirus says it is malicious.

The Five Best Password Managers

A while ago, all it took to be a great password manager was to keep your passwords in an encrypted vault. Now the best password managers give you the option to sync or keep them local only, change web passwords with a click, log in to sites for you, and more.

This story originally ran in January, 2015, and was updated with additional reporting from Patrick Austin in August 2017.

Back in 2015, we asked you to tell us which password managers you thought were the best, and pulled the five most popular options recommended by our readers. Since then, some have remained the same, some have updated their look, and some have undergone some pretty substantial changes, fundamentally altering the way they work and the features that appealed to users, for better or worse.

LastPass

LastPass is clearly the juggernaut here, and for good reason. The service was one of the first well-rounded password managers available, and one of the first that really made it

easy to store all of your passwords either online and synced with other computers and devices, or locally on one device. In short, LastPass remembers your passwords so you don't have to, and makes it easy to audit your passwords, use stronger passwords in general, and even automatically change a password for you if a service has been hacked or compromised. LastPass supports two-factor authentication for your password vault using Google Authenticator, USB devices (using a method we've outlined before), or a YubiKey. The service recently received a visual refresh to streamline the UI and make it easier to use, and sports a number of additional features like credit monitoring, secure password and document storage (and sharing), notifications when a site you have an account with has been hacked, tools to autofill forms and streamline online shopping, and more. LastPass supports Windows, macOS, Linux, Android, iOS, and Windows Phone, and has plugins for Chrome, Firefox, Safari, Opera, and Microsoft Edge.

While the company advises against it, you can download older versions of LastPass compatible with your device. LastPass is free to use on all your devices, including your smartphones, without imposing restrictions. For $24 a year, you can sign up for LastPass Premium. Premium features include priority customer support, 1GB of encrypted file storage (for sensitive info like scanned documents), Windows fingerprint reader support, and two-factor authentication either with a Yubikey or a thumb drive with Sesame.

Dashlane

Dashlane launched in beta back in 2012, debuted a UI refresh in 2016, and has since risen to prominence largely because of its attention to its interface (which is sharp and easy to use), simple security, easy auto-login, form auto-fill, and logging of purchases and orders from online shops. It's picked up a number of updates since then, including support for two-factor authentication, the ability to share passwords with emergency contacts in case you can't access your accounts, and the ability to change multiple passwords on dozens of websites with a few clicks. Dashlane will also notify you if you have an account on a site that's hacked, and with its built-in password changer, you can have Dashlane reset the password to a new, unique, strong one without leaving the interface. If you want to change all your passwords at once, you can do that too. The purchase tracking and digital wallet features make it easy to make online purchases even at retailers you don't have accounts with, and search all of your online orders in one place, while secure note and document sharing gives you a place to store passwords that can't be automatically filled in. Dashlane also gives you the option to store your passwords locally only in an encrypted vault (where only you have the master key), or to sync them to your devices and access them on the web. Dashlane supports Windows, macOS, Android, and iOS, and has plugins for Chrome, Firefox, Safari, and Internet Explorer. It's free to download and use, but if you want your passwords synced across devices, you'll need Dashlane Premium, at $40/yr.

KeePass

If free (as in speech and as in beer) and open source are your go-to requirements for a security product, KeePass is perfect for you. Your passwords in KeePass are stored inside an encrypted database that you control, on your own system, and are never synced or uploaded anywhere unless you want to take them from machine to machine. KeePass is also a portable app, meaning it's super easy to take with you and use on multiple computers, even if that machine is locked down and all you have is a thumb drive. It has its own password generator, to help you change passwords and make sure every one of them is unique and strong. Password databases in KeePass can also be configured with multiple keys so you can share access among privileged users, and exported in plain text for quick importing elsewhere (or backups). You can even create physical password keys in the form of thumb drives or CDs (even floppy disks if you want to go retro). Plus, KeePass has tons of third-party plugins and tools to extend its functionality and bring it to more devices, browsers, and platforms. Most notably, KeePass' auto-type functionality works in all windows and all browsers, which means that KeePass can log in to sites that other password managers can't, and can log in to applications, system dialogs, and other password prompts that you'd otherwise have to copy/paste a password into.

1Password

1Password is well-loved and well-regarded for offering a powerful and secure password manager and digital wallet in a really sharp-looking package that shines on every platform it runs on. It's flexible, easy to use, works seamlessly in just about every web browser, and packs in the same features that you've come to expect from a premium password manager and secure document storage tool. 1Password looks great, comes with a strong password generator to help you pick good passwords every time you change one, secure notes for other passwords or notes that you want to keep private, a digital wallet for bank accounts and payment info, and a password "recipe" builder that lets you customize your passwords to your demands instead of just accepting whatever algorithm the password generator spits out at you. Recently 1Password moved from a one-time purchase to a subscription based business model ($2.99 per month for an individual account, $4.99 per month for a family account supporting five people), and is now storing your encrypted password vault in its own cloud storage service. While it may be inconvenient for users who would prefer to locally store their files, according to engineers at 1Password's company AgileBits, it's more secure than syncing data with third-party storage options like iCloud and Dropbox. Older 1Password users can still use their cloud-synced vaults. If you're desperate for local vault storage, the company hasn't disabled it completely, and you can send them an email to discuss different vault storage options with a 1Password

member. You can also set up an emergency kit as a safety net and share passwords with authorized users. You can even keep multiple vaults for different types of passwords. 1Password supports Windows, macOS, Android, and iOS, with plugins for Chrome, Firefox, Opera, and Safari.

VPN Services

ExpressVPN

- Number of IP addresses: 30,000
- Number of servers: 3,000+
- Number of server locations: 160
- Number of simultaneous connections: 5
- Country/Jurisdiction: British Virgin Islands
- 94+ countries
- 3 months Free with 1-year plan

ExpressVPN also offers a 30-day money-back guarantee, and has impressive protocol support. While few will use PPTP (unless there are specific needs), the added support of SSTP and L2TP/IPSec may be welcome to some users.

We like the quality of their setup guides, and the detailed information in their FAQ. The ExpressVPN gained points from us for their support of Bitcoin as a payment method, and their reliable and easy-to-use connection kill switch feature.

The company has been in business since 2009, and has a substantial network of fast VPN servers spread across 94 countries. Their best plan is priced at just $6.67 per month for an annual package which includes 3 months free. ExpressVPN's commitment to privacy is a standout feature.

NordVPN

- Number of IP addresses: 5,000
- Number of servers: 5000+ servers
- Number of server locations: 61
- Country/Jurisdiction: Panama
- 60+ countries
- $2.99/month (75% discount) for a 3-year plan
- NordVPN in-depth review and hands-on testing

NordVPN is one of our top-performing VPN providers. They even offer a generous simultaneous connection count, with six simultaneous connections through their network, where nearly everyone else offers five or fewer.

NordVPN's network isn't as large as some of their competitors, so if you're trying to obfuscate your tracks, you might want a company with more servers. Otherwise, this company is clearly providing a winning offering.

Their best plan is 1-year subscription plan: $6.99 ($83.88). While their monthly price of $11.95 is at the high end of the spectrum, their yearly price of $83.88 is lower than most our contenders. And yes, they also have a full 30-day refund policy. NordVPN also offers a dedicated IP option, for those looking for a different level of VPN connection. They do offer $2.99/month (75% discount) for a 3-year plan.

IPVanish VPN

- Number of IP addresses: 40,000+
- Number of servers: 900
- Number of server locations: 60
- Country/Jurisdiction: United States
- $4.87/month (60% discount) for a 1-year plan
- **Father's Day Sale**: Friday June 7th - Sunday June 17th -- All IPVanish plans 50% off!

A big win for IPVanish is the fact that the company keeps zero logs. Zero. We also like the company's stance towards privacy. They even provide support to EFF, the Electronic Frontier Foundation, a nonprofit at the front lines of protecting online privacy.

A unique feature of IPVanish, and one we're very intrigued by, is the VPN's support of Kodi, the open-source media streaming app that was once known as XBMC. Any serious media fan has used or built Kodi or XBMC into a media player, and the integrated IPVanish Kodi plugin provides access to media worldwide.

At $7.50/month and $58.49 for a year, they're obviously trying to move you towards their yearly program. We awarded the company kudos for Bitcoin support, and their money-back guarantee. We're a little disappointed that they only allow a 7-day trial, rather than a full 30-days. The company is generous, with five simultaneous connections. We also liked their connection kill switch feature, a must for anyone serious about remaining anonymous while surfing.

PureVPN

- Number of IP addresses: 300,000
- Number of servers: 2000
- Number of server locations: 180
- Country/Jurisdiction: Hong Kong
- $3.33/month (70% discount) for a 1-year plan

PureVPN does not log connection information. We like that they offer a 30-day refund policy. They got bonus points because, important for some of our readers, PureVPN supports bitcoin payments and you're going like their fast performance.

Also, you can grow with them. If after some time, you need to scale up to business-level plans, the company has offerings for growth. Pricing is middle-of-the-road,at $10.95 per month and $35,88 per year.

Finally, we like that PureVPN has both Kodi and a Chromebook solution called out right on their Web page. In addition, PureVPN earns the distinction of being the first VPN service we've seen to fully implement the GDPR.

CyberGhost VPN

- Number of IP addresses: 2,800
- Number of servers: over 3,700 worldwide
- Number of server locations: 115
- 24/7 support response
- $2.75/month (79% discount) for a 3-year plan

- CyberGhost in-depth review and hands-on testing

  CyberGhost has been around since 2011 and has come out strongly as a supporter of "civil rights, a free society, and an uncensored Internet culture." We really liked how the company specifically showcases, on their Web site, how folks normally prevented from accessing such important services as Facebook and YouTube can bring those services into their lives via a VPN.

  The company has solid Linux support, supports VPN via routers, and has a solution for the popular Kodi media player. They check off all the boxes on protocol support and get kudos for offering a connection kill switch feature, along with supporting P2P and BitTorrent in most countries.

  Still, the few extra dollars are worth it. We liked how the company offers custom app protection, IPV5 support and DNS, IP, and WebRTC leak prevention. CyberGhost also picked up points for preserving anonymity by not logging connection data.

StrongVPN

- Number of IP addresses: 59,500
- Number of servers: 689
- Number of server locations: 70
- $5.83/month (42% discount) for a 1-year plan

  StrongVPN blasts onto our favorites list with excellent infrastructure and decent price performance. As with our other favorites, StrongVPN has a strong no-logging policy.

Since VPN is all about protecting your privacy, that's a place the savvy VPN providers can pick up points.

Strong also picks up kudos for its large base of IP addresses, which also helps protect your anonymity. They have a solid collection of servers and worldwide locations. For those of you who need a dedicated IP, you can get one from the company, but you'll need to contact support to get help setting it up.

One of StrongVPN's strongest strengths is the company's network. They own and operate their entire network infrastructure, which means they have no externally-dictated limits on bandwidth or the type of traffic allowed on the network. This gives you the confidence that you'll be able to power through your work.

StrongVPN's monthly price of $10 is in the middle of the pack, but their yearly price of $69.99 is among the lowest of our contenders.

Norton Secure VPN

- Number of countries: 29
- Number of servers: 1500
- Number of server locations: 200
- Country/Jurisdiction: US
- $39.99 for the first 12 months

Symantec, long known for excellence in security products, has a relatively limited offering in its VPN product. It does not

support P2P or BitTorrent, it does not have a kill switch feature, and it does not support Linux, routers or set top boxes.

On the other hand, it's a VPN product from Symantec, a publicly-traded company with a clearly documented management team. In most software categories, this might not be a notable advantage, but in the VPN world, where most companies have shadowy management and impossible-to-track-down ownership structures, it's refreshing to know exactly who we're dealing with and know through independent sources (the company's annual filing, the SEC, and analyst reports) that the company is trustworthy and accountable.

Hotspot Shield

- Number of IP addresses: 50,000
- Number of servers: 2500
- Number of server locations: 26
- $2.99/month (77% discount) for a 3-year plan

HotSpot Shield is a product that has had some ups and downs in terms of our editorial coverage. Back in 2016, they picked up some very positive coverage based on founder David Gorodyansky comments about protecting user privacy. Then, in 2017, a privacy group accused the company of spying on user traffic, an accusation the company flatly denies. Finally, just this year, ZDNet uncovered a flaw in the

company's software that exposed users. Fortunately, that was fixed immediately.

So what are we to make of HotSpot Shield? Frankly, the controversy caused us to drop them from our directory for a while. But they approached us, made a strong case for their ongoing dedication to privacy, and we decided to give them another chance.

Here's the good news. They offer one of the best money-back guarantee we've seen for VPN services, a full 45-days. They support Windows, Mac, iOS, and Android, along with plugins for Chrome and Firefox. They also support routers and media players (but not Linux). And, as a bonus, they have a connection kill switch feature.

The company does not support P2P or BitTorrent – and they also don't support the OpenVPN. Every other vendor does, but HotSpot Shield limits its protocol support to L2TP/IPSec and something they call Hydra, an enhancement of the transport protocol.

Overall, the company did impress us with their attention to privacy. They have a published privacy canary. They also told us, "We have built in malware, phishing and spam protection. Our commitment to our users is that Hotspot Shield will never store, log, or share your true IP address."

Hide My Ass

- Number of IP addresses: 3,106
- Number of servers: 830
- Number of server locations: 280

- Country/Jurisdiction: United Kingdom
- $2.99/month for 3-year plan

  We have to give these folks an extra shout-out just for the name of their service. The firm has a strong network with a good selection of protocols supported. While they have an extensive (and very clearly written set of policy documents), the company explicitly allows P2P and torrents.

  We like how HMA offers support on a wide range of devices including game consoles. We gave them kudos for bitcoin support, and their excellent money-back guarantee. They did make us frown a bit because they do log connection data. They also offer five simultaneous connections.

  While their monthly pricing of $11.52 is at the high end of the spectrum, their yearly pricing is competitive at $78.66 for a full year.

Virtual Private Networks

VPNs are really easy to use, and they're considered to be highly effective tools. They can be used to do a wide range of things. The most popular types of VPNs are remote-access VPNs and site-to-site VPNs.

What is a remote-access VPN?

A remote-access VPN uses public infrastructure like the internet to provide remote users secure access to their network. This is particularly important for organizations and their corporate networks. It's crucial when employees connect to a public hotspotand use the internet for sending work-related emails. A VPN client, on the user's computer or mobile device connects to a VPN gateway on the company's network. This gateway will typically require the device to authenticate its identity. It will then create a network link back to the device that allows it to reach internal network resources such as file servers, printers and intranets, as if it were on the same local network.

It usually relies on either Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL) to secure the connection. However, SSL VPNs can also be used to supply secure access to a single application, rather than an entire internal network. Some VPNs also provide Layer 2 access to the target network; these will require a tunneling protocol like PPTP (Point-to-Point Tunneling Protocol) or L2TP (Layer 2 Tunneling Protocol) running across the base IPsec connection.

What is a site-to-site VPN?

This is when the VPN uses a gateway device to connect to the entire network in one location to a network in another location. The majority of site-to-site VPNs that connect over the internet use IPsec. Rather than using the public internet, it is also normal to use career multiprotocol label switching (MPLS) clouds as the main transport for site-to-site VPNs.

VPNs are often defined between specific computers, and in most cases, they are servers in separate data centers. However, new hybrid-access situations have now transformed the VPN gateway in the cloud, typically with a secure link from the cloud service provider into the internal network.

What is a mobile VPN?

A traditional VPN can affect the user experience when applied to wireless devices. It's best to use a mobile VPN to avoid slower speeds and data loss. A mobile VPN offers you a high level of security for the challenges of wireless communication. It can provide mobile devices with secure access to network resources and software applications on their wireless networks. It's good to use when you're facing coverage gaps, inter-network roaming, bandwidth issues, or limited battery life, memory or processing power.

Mobile VPNs are designed and optimized to ensure a seamless user experience when devices are switching networks or moving out of coverage. It generally has a smaller memory footprint, and because of that, it also requires less processing power than a traditional VPN. Therefore, it enables your applications to run faster while the battery pack is able to last longer.

A Mobile VPN is a worthwhile tool to have since it increases privacy, user satisfaction and productivity, while also reducing unforeseen support issues caused by wireless connectivity problems. The increasing usage of mobile devices and wireless connectivity make it more important to ensure that your data is being transferred through a secure network. It will allow you to access the internet, while staying safe behind a firewall that protects your privileged information.

Who needs a VPN?

Individuals that access the internet from a computer, tablet or smartphone will benefit from using a VPN. A VPN service will always boost your security by encrypting and anonymizing all of your online activity. Therefore, both private and business users can benefit from using a VPN. Communications that happen between the VPN server and your device are encrypted, so a hacker or website spying on you wouldn't know which web pages you access. They also won't be able to see private information like passwords, usernames and bank or shopping details and so on. Anyone that wants to protect their privacy and security online should use a VPN.

How to choose a VPN Service?

There's a vast range of VPN servers on the internet. Some are free, but the best ones require a monthly subscription. Before you decide to download a VPN, make sure you consider these factors for understanding a VPN:

Cost - VPNs aren't too pricey, but they vary from vendor to vendor. If your main concern is price, then go with something

inexpensive, or free - like Spotflux Premium VPN or AnchorFree HotSpot Shield Elite. By all means, try a free server but they do have a few drawbacks since they attract a lot of users. Free servers are often slower, and since most are ad-supported, they place adverts on the online pages you access. Others can even limit the speed of your connection, as well as your online time or amount of data transferred.

It's also important to note that leading VPN providers such as NordVPN and Privacy Internet Access offer stronger security features to ensure you're digitally safe. When selecting a paid VPN service, always be sure to check which countries it operates servers in.

Reliability - Select a VPN that is reliable and read the reviews to make sure that it's capable of protecting you by providing you with sufficient online privacy.

High security - An effective VPN will have the following security features: 128-bit encryption, anonymous DNS servers and an absence of connection logs.

Are there any bandwidth limits? This can often be linked to price; paying more will generally provide more bandwidth with faster internet access.

Are apps for Android, iOS phones and tablets available? Apps for Android and iOS devices are also vulnerable, so make sure your VPN server can support them.

To ensure privacy, you want to make sure you have a VPN that doesn't store online logs. Some servers provide virus

and spyware protection, and features like that can significantly increase your online safety.

Using a no-logs VPN service will provide you with a higher degree of security. It can protect you from blanket government surveillance and prevent your internet service provider from knowing your online activity.

Using a VPN for Netflix and other forbidden treasures

Online streaming services like Netflix and Hulu have been making it difficult for foreign users to access their content in other countries. Many people can get around region restrictions by using a VPN service to route your traffic through another country.

It can be quite simple to watch Netflix and other restricted goodies. You'll have to use a VPN service that allows you to get a unique IP address. This can often be available for an additional fee. Look for VPN services that offer a "dedicated IP address", "dedicated IP", or "static IP." Additional features like these will always allow you to access content from Netflix through a VPN service.

This is by far the easiest way to access your forbidden apps since there's no specific way to block VPN traffic.

A lot of people started using a VPN to evade geo-restrictions. But despite its forbidden benefits to users outside the US, a VPN is a great tool that can protect you and enhance your online experience over the internet by providing you with sufficient security and privacy. When it comes to selecting the best VPN, you have plenty of choices. There are many cost-effective VPN options, and all of them will vary in monthly offerings. Choosing the best