Staying Safe Online: A Practical Guide to Cybersecurity

By Curtis Jerry Smothers

Updated from an article originally written October 6, 2020

The Internet has become an indispensable part of everyday life. We bank, shop, communicate, work, learn, and entertain ourselves online. That convenience also gives criminals more opportunities to steal passwords, impersonate trusted organizations, infect computers, and trick ordinary people into giving away information.

Hackers, scammers, and cybercriminals use both sophisticated technology and old-fashioned deception. Fortunately, you don't have to be a cybersecurity expert to protect yourself. For the average computer user, staying safe online comes down to three things: **understanding the threats, strengthening your defenses, and protecting your Internet connection when necessary.**

1. Understand the Threats

Today's threats include phishing, malicious websites, ransomware, information-stealing malware, fraudulent text messages, fake technical-support warnings, account takeovers, and attacks that exploit previously unknown software vulnerabilities.

Yet one thing has remained remarkably consistent: **the person sitting in front of the computer is often the criminal's easiest target.** Rather than trying to defeat sophisticated security technology, a scammer may simply persuade you to click a link, open an attachment, reveal a password, approve a login, or send money.

Awareness is therefore an important part of cybersecurity. Slow down when something unexpected appears on your screen, particularly when the message creates urgency, fear, curiosity, or excitement.

2. Be Wary of Browser-Based Attacks

The Internet has changed considerably since this article was originally written in 2020. Adobe Flash is gone, modern browsers are much better at isolating websites from the rest of the computer, and browsers such as Safari, Chrome, Edge, and Firefox receive frequent security updates.

Malicious websites haven't disappeared, however. A dangerous page may try to persuade you to download malware, install a questionable browser extension, allow unwanted notifications, enter credentials into a fake login screen, or call a fraudulent "technical support" number.

Keep your browser and operating system updated. Be suspicious of unexpected download buttons and alarming messages such as **"Your computer is infected—click here immediately."** Don't install software merely because a website tells you that you need it.

3. Understand What HTTPS Does—and Doesn't Do

The padlock and **HTTPS** in a browser indicate that information traveling between your device and the website is encrypted. That's important, particularly when entering passwords, financial information, or other private data.

But HTTPS does **not** prove that a website is trustworthy. Criminals can obtain HTTPS certificates for fraudulent websites too.

Instead of relying on the padlock alone, examine the website address carefully. For banking, shopping, medical, and other sensitive accounts, use a bookmark, trusted app, or an address you know rather than following a link in an unexpected email or text.

4. Protect Your Online Accounts

Logging out of sensitive accounts when you're finished remains a sensible practice, particularly on shared or public computers. More important, however, is protecting the account itself.

Use a unique password for every important account and enable **multifactor authentication (MFA)** whenever possible. That way, stealing your password alone may not be enough for an intruder to get in.

For your most important accounts, consider **passkeys** when they are offered. Passkeys can provide excellent protection against phishing because they are tied to the legitimate website or app and cannot simply be typed into a convincing fake login page.

5. Be Careful What You Share on Social Media

Social media can provide criminals with a surprising amount of information. Birthdays, family names, pets, workplaces, vacation plans, photographs, and personal histories can all help a scammer construct a convincing message.

Review your privacy settings and think before posting information that could help someone impersonate you or answer account-recovery questions.

This doesn't mean you need to disappear from social media. It simply means recognizing that information you publish may be seen by people you never intended to see it.

6. Don't Get Hooked by Phishing

Phishing remains one of the most successful forms of cybercrime because it exploits human behavior rather than computer technology.

A typical message might say:

"Your account has been compromised. Verify your information immediately."

The link leads to a fake website that looks remarkably similar to the real one. When the victim enters a username and password, the information goes directly to the criminal.

Variations include **spear phishing**, which uses information about a particular victim; **business email compromise**, in which criminals impersonate executives, vendors, or coworkers to request money or sensitive information; and **smishing**, which delivers the same sort of deception through text messages.

When an unexpected message asks you to sign in, don't use its link. Open the organization's app or website independently and check your account there.

7. Use Your Computer's Built-In Security

The advice to "install antivirus software" has also changed since 2020.

Modern versions of Windows include Microsoft Defender, firewall protection, malware detection, and other security features. Macs include built-in technologies such as Gatekeeper, XProtect, FileVault encryption, and a firewall.

For many home users, keeping these built-in protections enabled and the operating system updated provides a strong foundation. Commercial security software can add useful features, but buying another antivirus program is no longer automatically necessary for everyone.

Whatever protection you use, **keep it updated**. Security software cannot defend against newly discovered threats if its defenses are years out of date.

8. Be Sensible About Public Wi-Fi

Public Wi-Fi deserves caution, but it isn't quite the digital minefield it once was. Because most reputable websites and apps now encrypt their traffic with HTTPS, simply connecting to a hotel, airport, coffee-shop, or library Wi-Fi network does not automatically expose everything you do.

Still, avoid unknown or suspicious networks. A criminal can create a convincing network name such as "Airport Free WiFi" and hope travelers connect to it.

For sensitive activity, your cellular connection or personal hotspot is an excellent alternative. A reputable VPN can provide an additional encrypted layer on an untrusted network, particularly when traveling.

9. Use Long, Unique Passwords—and a Password Manager

One of the most important changes in password advice is that **length and uniqueness matter more than forcing yourself to invent complicated passwords you cannot remember.**

Don't reuse passwords. If one company suffers a data breach, criminals routinely try stolen passwords on other websites.

A password manager can create and store long, random passwords so you don't have to memorize dozens of them. Apple's Passwords app, browser password managers, and reputable third-party password managers can all make good password hygiene much easier.

For passwords you do need to remember, a long and unusual passphrase can be easier to remember and harder to guess than a short jumble of characters.

Also, avoid relying on security questions such as your mother's maiden name or the city where you were married. Much of that information can be discovered online. MFA and passkeys are much stronger alternatives.

10. Back Up Everything

This advice hasn't changed: **Back up your important files.**

Ransomware, hardware failure, theft, accidental deletion, software corruption, and simple human error can all destroy valuable information. A good backup turns a catastrophe into an inconvenience.

Use more than one backup when the information is irreplaceable. A local external drive provides fast recovery, while a separate or offsite backup protects against theft, fire, and other disasters.

Most importantly, don't leave your only backup permanently exposed to the computer it protects. Malware and ransomware can sometimes attack connected storage too. An encrypted backup drive that can be disconnected when it isn't being used provides another layer of protection.

Where Does a VPN Fit In?

A **Virtual Private Network (VPN)** creates an encrypted connection between your device and the VPN provider's server. It can conceal your public IP address from the websites you visit, reduce what the local network can observe, and provide useful protection when using unfamiliar networks.

But a VPN is **not an antivirus program, a phishing blocker, or an invisibility cloak.**

If you voluntarily enter your password into a fraudulent website, a VPN cannot save you. If you download malware, the VPN doesn't magically remove it. And although the VPN prevents your Internet provider from seeing some of your browsing activity, you are shifting a degree of trust to the VPN provider.

Choose a reputable provider with clear privacy policies rather than an unknown "free VPN" whose business model may depend on advertising or collecting user information.

The Bottom Line

Cybersecurity doesn't require living in fear of the Internet. It requires developing good habits.

Keep your computer, phone, browser, and applications updated. Use unique passwords, a password manager, MFA, and passkeys where available. Treat unexpected messages and links with suspicion. Protect sensitive personal information. Maintain reliable backups and disconnect backup drives when practical. Be cautious on unfamiliar networks, and use a reputable VPN when its additional privacy protection is useful.

Most cybercriminals are looking for the easiest target. A few sensible precautions can make you a much more difficult one.

As the desk sergeant used to remind the officers heading onto the streets in *NYPD Blue*:

Be careful out there.

STAY SAFE ONLINE

A 3-PRONGED APPROACH TO CYBERSECURITY

Knowledge, smart habits, and a VPN are your best defense against today's online threats.

THE 3-PRONGED APPROACH

1 THREAT AWARENESS

Understand today's threats like phishing, malware, social engineering, and sophisticated attacks.

2 SHORING UP DEFENSES

Use smart security habits and built-in protections to safeguard your data and devices.

3 STAY OFF THE THREAT RADAR WITH A VPN

Encrypt your connection, mask your IP, and browse privately—especially on public Wi-Fi.

Cybercriminals are always looking for a way in.
Stay informed. Stay protected. Stay safe.

REMEMBER

- BACK UP EVERYTHING
- USE STRONG PASSWORDS
- AVOID PUBLIC WI-FI
- KEEP SOFTWARE UP TO DATE

Staying Safe Online: A Practical Guide to Cybersecurity

By Curtis Jerry Smothers

Updated from an article originally written October 6, 2020

The Internet has become an indispensable part of everyday life. We bank, shop, communicate, work, learn, and entertain ourselves online. That convenience also gives criminals more opportunities to steal passwords, impersonate trusted organizations, infect computers, and trick ordinary people into giving away information.

Hackers, scammers, and cybercriminals use both sophisticated technology and old-fashioned deception. Fortunately, you don't have to be a cybersecurity expert to protect yourself. For the average computer user, staying safe online comes down to three things: **understanding the threats, strengthening your defenses, and protecting your Internet connection when necessary.**

1. Understand the Threats

Today's threats include phishing, malicious websites, ransomware, information-stealing malware, fraudulent text messages, fake technical-support warnings, account takeovers, and attacks that exploit previously unknown software vulnerabilities.

Yet one thing has remained remarkably consistent: **the person sitting in front of the computer is often the criminal's easiest target.** Rather than trying to defeat sophisticated security technology, a scammer may simply persuade you to click a link, open an attachment, reveal a password, approve a login, or send money.

Awareness is therefore an important part of cybersecurity. Slow down when something unexpected appears on your screen, particularly when the message creates urgency, fear, curiosity, or excitement.

2. Be Wary of Browser-Based Attacks

The Internet has changed considerably since this article was originally written in 2020. Adobe Flash is gone, modern browsers are much better at isolating websites from the rest of the computer, and browsers such as Safari, Chrome, Edge, and Firefox receive frequent security updates.

Malicious websites haven't disappeared, however. A dangerous page may try to persuade you to download malware, install a questionable browser extension, allow unwanted notifications, enter credentials into a fake login screen, or call a fraudulent "technical support" number.

Keep your browser and operating system updated. Be suspicious of unexpected download buttons and alarming messages such as **"Your computer is infected—click here immediately."** Don't install software merely because a website tells you that you need it.

3. Understand What HTTPS Does—and Doesn't Do

The padlock and **HTTPS** in a browser indicate that information traveling between your device and the website is encrypted. That's important, particularly when entering passwords, financial information, or other private data.

But HTTPS does **not** prove that a website is trustworthy. Criminals can obtain HTTPS certificates for fraudulent websites too.

Instead of relying on the padlock alone, examine the website address carefully. For banking, shopping, medical, and other sensitive accounts, use a bookmark, trusted app, or an address you know rather than following a link in an unexpected email or text.

4. Protect Your Online Accounts

Logging out of sensitive accounts when you're finished remains a sensible practice, particularly on shared or public computers. More important, however, is protecting the account itself.

Use a unique password for every important account and enable **multifactor authentication (MFA)** whenever possible. That way, stealing your password alone may not be enough for an intruder to get in.

For your most important accounts, consider **passkeys** when they are offered. Passkeys can provide excellent protection against phishing because they are tied to the legitimate website or app and cannot simply be typed into a convincing fake login page.

5. Be Careful What You Share on Social Media

Social media can provide criminals with a surprising amount of information. Birthdays, family names, pets, workplaces, vacation plans, photographs, and personal histories can all help a scammer construct a convincing message.

Review your privacy settings and think before posting information that could help someone impersonate you or answer account-recovery questions.

This doesn't mean you need to disappear from social media. It simply means recognizing that information you publish may be seen by people you never intended to see it.

6. Don't Get Hooked by Phishing

Phishing remains one of the most successful forms of cybercrime because it exploits human behavior rather than computer technology.

A typical message might say:

"Your account has been compromised. Verify your information immediately."

The link leads to a fake website that looks remarkably similar to the real one. When the victim enters a username and password, the information goes directly to the criminal.

Variations include **spear phishing**, which uses information about a particular victim; **business email compromise**, in which criminals impersonate executives, vendors, or coworkers to request money or sensitive information; and **smishing**, which delivers the same sort of deception through text messages.

When an unexpected message asks you to sign in, don't use its link. Open the organization's app or website independently and check your account there.

7. Use Your Computer's Built-In Security

The advice to "install antivirus software" has also changed since 2020.

Modern versions of Windows include Microsoft Defender, firewall protection, malware detection, and other security features. Macs include built-in technologies such as Gatekeeper, XProtect, FileVault encryption, and a firewall.

For many home users, keeping these built-in protections enabled and the operating system updated provides a strong foundation. Commercial security software can add useful features, but buying another antivirus program is no longer automatically necessary for everyone.

Whatever protection you use, **keep it updated**. Security software cannot defend against newly discovered threats if its defenses are years out of date.

8. Be Sensible About Public Wi-Fi

Public Wi-Fi deserves caution, but it isn't quite the digital minefield it once was. Because most reputable websites and apps now encrypt their traffic with HTTPS, simply connecting to a hotel, airport, coffee-shop, or library Wi-Fi network does not automatically expose everything you do.

Still, avoid unknown or suspicious networks. A criminal can create a convincing network name such as "Airport Free WiFi" and hope travelers connect to it.

For sensitive activity, your cellular connection or personal hotspot is an excellent alternative. A reputable VPN can provide an additional encrypted layer on an untrusted network, particularly when traveling.

9. Use Long, Unique Passwords—and a Password Manager

One of the most important changes in password advice is that **length and uniqueness matter more than forcing yourself to invent complicated passwords you cannot remember.**

Don't reuse passwords. If one company suffers a data breach, criminals routinely try stolen passwords on other websites.

A password manager can create and store long, random passwords so you don't have to memorize dozens of them. Apple's Passwords app, browser password managers, and reputable third-party password managers can all make good password hygiene much easier.

For passwords you do need to remember, a long and unusual passphrase can be easier to remember and harder to guess than a short jumble of characters.

Also, avoid relying on security questions such as your mother's maiden name or the city where you were married. Much of that information can be discovered online. MFA and passkeys are much stronger alternatives.

10. Back Up Everything

This advice hasn't changed: **Back up your important files.**

Ransomware, hardware failure, theft, accidental deletion, software corruption, and simple human error can all destroy valuable information. A good backup turns a catastrophe into an inconvenience.

Use more than one backup when the information is irreplaceable. A local external drive provides fast recovery, while a separate or offsite backup protects against theft, fire, and other disasters.

Most importantly, don't leave your only backup permanently exposed to the computer it protects. Malware and ransomware can sometimes attack connected storage too. An encrypted backup drive that can be disconnected when it isn't being used provides another layer of protection.

Where Does a VPN Fit In?

A **Virtual Private Network (VPN)** creates an encrypted connection between your device and the VPN provider's server. It can conceal your public IP address from the websites you visit, reduce what the local network can observe, and provide useful protection when using unfamiliar networks.

But a VPN is **not an antivirus program, a phishing blocker, or an invisibility cloak.**

If you voluntarily enter your password into a fraudulent website, a VPN cannot save you. If you download malware, the VPN doesn't magically remove it. And although the VPN prevents your

Internet provider from seeing some of your browsing activity, you are shifting a degree of trust to the VPN provider.

Choose a reputable provider with clear privacy policies rather than an unknown "free VPN" whose business model may depend on advertising or collecting user information.

The Bottom Line

Cybersecurity doesn't require living in fear of the Internet. It requires developing good habits.

Keep your computer, phone, browser, and applications updated. Use unique passwords, a password manager, MFA, and passkeys where available. Treat unexpected messages and links with suspicion. Protect sensitive personal information. Maintain reliable backups and disconnect backup drives when practical. Be cautious on unfamiliar networks, and use a reputable VPN when its additional privacy protection is useful.

Most cybercriminals are looking for the easiest target. A few sensible precautions can make you a much more difficult one.

As the desk sergeant used to remind the officers heading onto the streets in *NYPD Blue*:

Be careful out there.