Call us:
800.545.4442

Email us:
info@towneley.com

Visit us online:
www.towneley.com

SEPTEMBER 8, 2021

# PROTECT YOURSELF FROM IDENTITY THEFT AND CYBERCRIME (3-PART SERIES)

## Part 2: Protecting Your Computer and Online Accounts

**This Article Is the Second in a 3-part series on protecting yourself and your loved ones from identity theft and cybercrime.**

- Part 1 outlined some steps you can take to protect your identity.
- Part 2 focuses on protecting your computer and online accounts from cybercriminals.
- Part 3 identifies clever tricks and scams to avoid.

As we learned in Part 1, diligently protecting your personal information is one of your best defenses against identity theft. Unfortunately, many identity thieves are not satisfied with using stolen social security and financial account numbers to wreak havoc – they have also become adept at using your technology against you. Tech-savvy fraudsters are using crafty techniques to hack their way into unsuspecting victims' computers, phones, and social media accounts to steal and exploit their private information.

This paper discusses various ways to protect yourself, your computer, and your online accounts from cybercriminals who leverage technology to steal your identity.

### Protecting Yourself While Surfing the Internet

**Use Anti-Virus Software and Run Security Updates**

The first step to securing your computer (or tablet or smartphone) is keeping your device's operating system and antivirus software up to date. If you run a Windows operating system on your computer or other devices, you should also have updated antivirus software installed to block malware from infecting your computer. Malware is short for "malicious software," specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

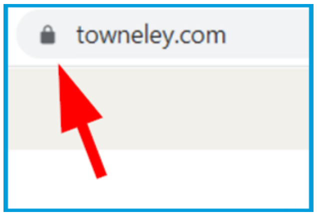
Some popular antivirus software options are McAfee, Norton, and Trend Micro. Another option, Windows Defender, is included with Windows 10. In addition to keeping your antivirus software up to date, it's also good practice to check regularly for operating system updates (Windows, iOS, etc.) so that you'll be able to have the manufacturer's latest security patches directly installed.

However, keep in mind that antivirus programs only provide one layer of perimeter security. If your computer becomes infected by malware that evades your antivirus software, you'll need a second line of defense. In that case, consider installing a separate malware removal program whose sole purpose is to seek and destroy nefarious software on your computer. One such option is Malwarebytes, a popular free program that runs alongside your antivirus software.

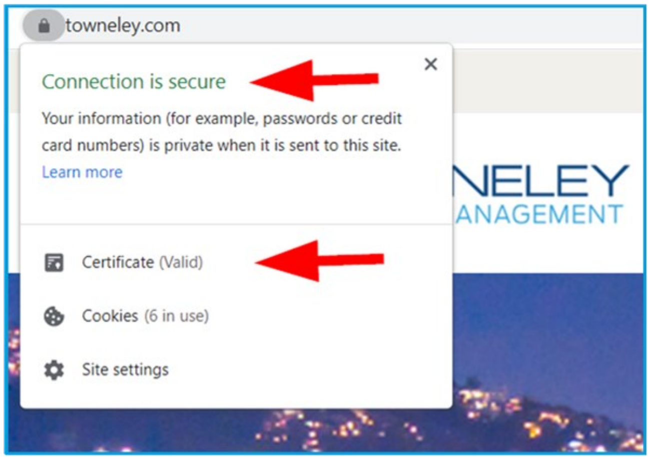
### Protect Your Login Credentials

If a malicious person successfully gains access to your login credentials for one of your financial accounts, that person can take over the account and lock you out by changing your username and password. This form of identity theft is called an account takeover. Once they have access to your account, the fraudster can change account details, steal financial information, and possibly even place transactions or withdraw funds. Therefore, carefully protect your account login credentials. Don't use the same login and password for different accounts and change your credentials periodically. Also, if the provider offers multi-factor authentication, opt-in to that service (more about that below).

Another safe internet practice is to always log in to websites directly by typing in the URL or through a previously bookmarked link you know is safe. Don't access the website by clicking on a link in an email or pop-up window. And, before you start entering your personal information (username, password, billing info, etc.), make sure that you are on a secure site by looking for a padlock icon at the beginning of the web address.


towneley.com

When in doubt, or for further authentication, click on the padlock icon to view the digital security certificate, which verifies the website's authenticity.


towneley.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Certificate (Valid)

Cookies (6 in use)

Site settings

### Update and Back Up Your Computer (Regularly!)

You'll want to configure your computer's settings so that both your operating system software and your antivirus software update automatically. In addition, you should back up important files on your hard drive regularly so you can recover them if, for example, you lose data during a ransomware attack. While the best way to back up your computer files is to an external hard drive, you can also back up your files automatically to a cloud storage service, such as Dropbox, Google Drive, Microsoft OneDrive, and iCloud for iOS users.

### Protect Your Home Wi-Fi Network

With everyone working and schooling from home these days, in addition to streaming movies and gaming online for entertainment, we are using our home Wi-Fi networks more than ever before. And cybercriminals are having a field day. Once they crack your wireless network's security protocols, Wi-Fi hackers can view, store, and download all data sent via the network. Hackers can also attack the network itself or go after any of your family's connected devices (they'll pick whichever one is the weakest link). They can then use your posts, saved files, and other data to compromise passwords and reveal information about where you work or travel. The hackers can even deploy a ransomware attack to intimidate you into paying them money to release your stolen information.

Thankfully, there are a few easy steps you can take to protect your home network. First, change your Wi-Fi's default name to make it harder for hackers to know what type of router you have. You'll also want to change the default username and password for your router, as that's usually easy for hackers to guess, especially if they know the router's manufacturer. Additionally, when changing your Wi-Fi password, make sure that you use a strong passphrase (more on that later) and set your router's encryption standard to WPA2 (the most secure option at this time).

Also, as an added precaution when children are actively using Wi-Fi, consider purchasing a separate router for the kids' devices. That way, if a hacker does gain access to the kids' network, they won't also have access to the parents' personal information.

### Use A Virtual Private Network (VPN)

A virtual private network, or VPN, adds a layer of protection to your online activities by building an encrypted tunnel between your network traffic and anyone trying to spy on you. In simple terms, it creates a secure connection between your computer and the websites you are visiting. A VPN is a must when accessing sensitive information on a public Wi-Fi network, and it provides an added layer of security to your home Wi-Fi network.

There are several VPN options to choose from – make sure you check the reviews and get one that encrypts all internet traffic. And, if you don't have a VPN? Instead of using a public Wi-Fi network, it's safer to use the cellular network on your mobile phone to connect to the internet – it'll be more secure.

### Beware Of Pop-Ups

Ethan Zuckerman is known as one of the creators of the online pop-up ad. These ads are focused on attracting internet traffic, which is why they annoyingly "pop up" in front of the page you are currently viewing online. The advertisers behind these pop-up ads are hoping that you'll inadvertently click on the pop-up ad, go to their website, and buy whatever they are selling.

CONGRATULATIONS!

You've been chosen to receive a FREE Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE Desktop Computer!

Click OK to download our free software while browsing the site

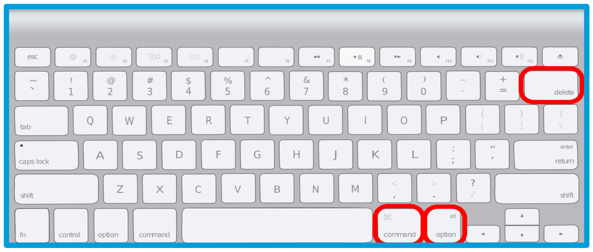
In his August 2014 essay for *The Atlantic* titled "The Internet's Original Sin", Zuckerman publicly apologized (perhaps tongue-in-cheek, perhaps not) for writing the code that gave pop-up ads life. He stated, "At the end of the day, the business model that got us funded was advertising. The model that got us acquired was analyzing users' personal homepages so we could better target ads to them. Along the way, we ended up creating one of the most hated tools in the advertiser's toolkit: the pop-up ad."

Be wary of pop-ups, as they're not always what they seem to be. For example, be particularly suspicious of pop-ups that encourage you to download a video, or inform you that you're the lucky winner, or inform you that your computer is infected, with instructions to immediately call the number on the screen for assistance. Don't ever click on anything in these pop-ups, including the "X" inside the pop-up window itself or buttons that say: "No Thanks," "Close," or "Leave Page" – those are attempts to trick you. Clicking anywhere on the box might download a virus that infects your device or could implant a keylogger that tracks everything you type on your keyboard, including usernames and passwords.

Instead, to remove the pop-up ad safely, start by holding down three keys: CTL + ALT + DEL (Windows) or CMD + Option + Escape (Mac). Select the browser window(s) you want to close, then click "End Task" (Windows) or "Force Quit" (Mac). Lastly, run your antivirus software to make sure there isn't any malware on your computer that launched the pop-up ad in the first place.

> "Along the way, we ended up creating one of the most hated tools in the advertiser's toolkit: the pop-up ad."

CTL + ALT + DEL (Windows)



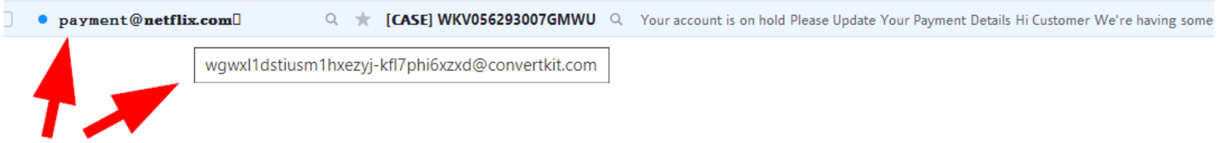
CMD + Option + Escape (Mac)

## Protecting Yourself While Using Email

### Hover To Discover

Before opening just any email that arrives in your inbox, you should be aware that cyber thieves can easily spoof email addresses. A spoofed email appears to be coming from a sender that you recognize, but in fact, the sender's email address is "spoofed" with a fake sender address. The fraudsters know that people are more likely to trust incoming emails from names they recognize, making recipients more likely to unknowingly click malicious links, open malware attachments, and send sensitive data to the wrong people.

To determine if an email has been spoofed, hover your mouse over the sender's email address (without pressing or clicking) to identify the sender's actual email address. If the two email addresses are different, you know that someone is trying to trick you.

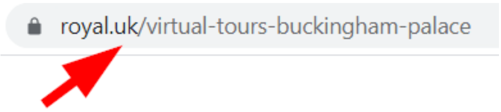


payment@netflix.com [CASE] WKV056293007GMWU Your account is on hold Please Update Your Payment Details Hi Customer We're having some

wgwxl1dstiusm1hxezyj-kfl7phi6xzxd@convertkit.com

Hovering also works with website links in the body of an email, so you can see what site the link will redirect you to before you click on it. To preview the link on a mobile device, press and hold the link to discover the actual web address.

Other clues to watch for are website links from foreign countries, as a foreign country code could indicate a possible fraud attempt. If you see two letters before the first single slash in a website link, those letters refer to the country where the domain name is registered. For example, this web address takes you to a website located in the United Kingdom:


royal.uk/virtual-tours-buckingham-palace

### Unsubscribe From Unwanted Emails

If you receive unwanted emails from organizations you know or have done business with previously, it's okay to unsubscribe from future emails by clicking the "Unsubscribe" link in the small print at the bottom of the email. However, make sure that you never unsubscribe from spam emails or senders that you don't recognize. That notifies the sender that you have an active email address (which will likely result in even more spam coming your way!). Instead, block the sender's email address or mark it as spam so that future emails are barred or moved directly to your spam folder.

## Protecting Yourself When Accessing Online Accounts

### Passphrases Are Stronger Than Passwords

Every online account requires you to enter a username and a password to log in. While you've likely heard by now that more complex passwords are safer from cyber-hacking than simple ones and that you should never use the same password for multiple sites, something you may not have thought of yet is using a passphrase instead of a password. A passphrase is like a password, except it's composed of several words strung together instead of just one word. Using a phrase as a password is easier to remember and makes it more difficult to hack.

To make a strong passphrase, use at least 12 characters (the more, the better). A long passphrase helps protect you against "brute force attacks," a type of hacking that relies on guessing possible combinations of your password (often with the assistance of software) until the hacker arrives at the correct sequence. The longer the passphrase, the more combinations to test.

It's also essential to never reuse the same passphrase for any of your online accounts. This practice helps defend against another nefarious technique called "credential stuffing." Credential stuffing is a type of cyberattack in which a crook uses a stolen username and password from one site to access your accounts at other sites. Cybercriminals can steal usernames and passwords via large-scale cyberattacks or purchase them off the dark web. Credential stuffing is one of the most successful cybercrime techniques because up to 65% of people reuse the same password for multiple accounts, and the fraudsters know it.

Instead, create a unique passphrase for each of your accounts. For example, if you're a big Humphrey Bogart fan, you could make your Netflix passphrase "hereslookingatyoukid." Or, a passphrase for one of your financial accounts might be "showmethemoney." If you have the option, add more complexity to your passphrase by incorporating a mixture of upper- and lower-case letters, numbers, symbols, and interchanging digits for letters, such as "$howmEtheM0neY".

### Use A Password / Passphrase Manager

A password manager is a software or app that securely stores your passwords and passphrases. Password managers make it easier to use and remember your unique passwords for each account, so you can avoid keeping a written list of your passwords next to your computer or in your wallet.

A good password manager stores and encrypts your passwords, generates new random passwords, and enables you to easily access your stored passwords from all your electronic devices. Some password manager options are Keeper, Dashlane, 1Password, LastPass, and Bitwarden.

### Use Multi-Factor Authentication When Possible

Today, many website sponsors (especially financial service providers, such as banks and credit card companies) require you to enable Multi-Factor Authentication (MFA) to access your account online. Also known as two-step verification, MFA is a security technology requiring the user to provide two or more forms of identity verification when logging in. Frequently, this includes a password or passphrase and a personal identification number (PIN). Typically, after you enter your username and password, the website sends a PIN to your phone (via text or call), which you must type in within a few minutes to complete the login process.

MFA helps prevent fraudsters from accessing your online accounts and is highly recommended for financial and email accounts and for accessing cloud storage services such as Dropbox.

## Protecting Your Social Media Accounts

### Keep Your Identity Safe on Social Media

These days just about everyone has at least one social media account. Unfortunately, scammers regularly steal people's social media identities by using personal information and photos copied from their Facebook, LinkedIn, Instagram, and Twitter accounts. Social media hackers use your profile to build a fake profile purporting to be yours. They'll then scam people out of money or post comments with viewpoints contrary to yours, tarnishing your reputation and saddling you with the chore of restoring your online identity.

To prevent this from happening, use caution when posting information about yourself on social media. Cybercriminals use personally identifying details such as your full name (middle name included), date of birth, hometown, pet names, interests, occupation and address to commit fraud. Protect this information as much as possible to thwart their efforts.

Be wary of friend requests from people you don't know, as the request may be coming from cyber-attackers posing as someone else. Also, be aware that the default sharing protocol for some social media sites is "Public." If selected, that setting means the public can see your posts, not just your friends. A safer bet is to change the default sharing option to "Friends," which will ensure that only your approved friends see your posts.

As we've learned, modern technology doesn't just bring convenience, efficiency, and all-around awesomeness to our busy lives — it also offers more opportunities than ever before to fraudsters seeking to steal and exploit our personal information for their own gain. Fortunately, by taking the prudent steps outlined above, you can help to ensure that your private electronic information remains private.

In our next and final installment (PART 3), we will discuss ways to identify common tricks and scams designed to steal your identity, your money, and your property. Stay tuned!