BY TRIONA GUIDRY

Wide web

A writer's guide to internet safety.

The internet may be a wealth of information for writers, but it can also be a heap of trouble. Your productive workday can easily derail thanks to a sneaky computer virus, a rogue link, or an infected ad.

Today's internet viruses are more aggressive than ever, commandeering your computer and charging cash ransoms for removal. Financial fraud and identity theft run rampant, fueled by hijacked social media accounts. Prevention is the key to keeping your data accessible when you need it. By using strong passwords and secure networks, you can stay safe while getting your work done.

Have you ever received a message from a friend that seemed suspicious? Maybe they claimed they were overseas and in need of help, or perhaps they urged you to click a strange-looking link. These are examples of account hijacking, when hackers break in, change the passwords, and then start sending viruses and spam. Not only is it a nuisance, it can be a blow to your professional reputation. Imagine having to explain to your editor that a hacker hijacked your account and is sending them malware!

Strong passwords are critical when protecting your accounts from hijacking. Passwords should be at least 12 characters long. They should contain a mix of upper- and lowercase letters with at least two numbers and two symbols. Even more important, your passwords need to be different for every single account. That may seem overwhelming, but password management tools such as 1Password, LastPass, and KeePass can help. These programs create secure password vaults and will help you generate strong passwords.

Now is a good time to change your passwords, as there have been a number of recent incidents at major sites. Don't just rotate through the same two or three passwords, though. Choose passwords that are brand new. Again, password management tools can help.

You should note that password management tools themselves are not invulnerable to hackers. Always keep written backups of your passwords in a locked place. Always install any updates to your password management software, and sign up for announcements so you can find out if the company has suffered any recent security incidents.

Unfortunately, passwords aren't the best method of protecting data no matter how strong they are. That's why sites are turning to two-factor authentication (2FA) or two-step verification (2SV). Two-factor authentication requires two methods of verification: your password, plus a one-time numeric code that is typically texted to your smartphone. Experts recommend using two-step authentication where available. If you enable it, be sure to store any backup codes in a safe place.

Many writers rely on public Wi-Fi when working at coffee shops or other public spaces, but open networks can be filthier than open sewers. You don't know what viruses could be lying in wait in the network, ready to infect your computer the moment you connect. Worse, someone sharing that network could be a thief running a so-called network sniffer. That's a program that "sniffs out" and records anything that isn't encrypted, including usernames, passwords, credit card numbers, and, yes, even your writing. To avoid this, you should either encrypt your connections – or avoid using public networks altogether.

One option to protect your information is to use a virtual private network, or VPN. A VPN creates a private "channel" between you and your destination website. While VPNs work well, they're not always easy to configure or troubleshoot. And it doesn't change the fact that you're still

lenoleum/Shutterstock

using a public network. If there's a bug in your VPN software or it's configured incorrectly, you could still be transmitting private data. Be sure to read the instructions carefully, make a backup of your computer data, and take note of your original network settings before you change them. And watch out for malware pretending to be VPN software. Only use legitimate VPN programs, and download directly from the manufacturer or app store to avoid lookalike fakes. Even if you use a VPN, you should never access your bank accounts or use your credit card over a public network. It's a risk that's just not worth taking.

One alternative to using public networks is to use a private Wi-Fi hotspot. Sometimes called a wireless tether, a personal hotspot is your own wireless network-on-the-go. Your smartphone may already have the capability to set up hotspots, although you may need to pay extra for the service. You can also purchase a separate device to create a hotspot. When you use a personal hotspot, you don't have to use public networks at all. You don't have to wonder if the place where you'll be working has public Wi-Fi. You're not sharing your connection unless you want to – although you should double-check to make sure your device isn't doing so by default.

Many writers rely on public Wi-Fi when working at coffee shops or other public spaces, but open networks can be filthier than open sewers.

Another dilemma is how to do online research without getting infected by computer viruses. Normally I recommend that people avoid clicking on links they don't know, but writers often have to do this in the name of research. So how can you mitigate your risks?

First, I suggest using a different web browser for research than the one you use for your bank accounts, and a separate third browser for social media. This divides your online activities and protects your more vulnerable financial accounts. The default Windows browser is Internet Explorer or Edge, and on Macs, it's Safari. You could use your default browser for research and, say, Chrome for banking and Opera for social media. You still need good antivirus software, but using multiple browsers will help you avoid account hijacking and bad links.

The research browser is your throwaway browser. Set it to open links by default, and don't log into your other accounts from it. It should be configured to use private windows, limit ad tracking, and automatically clear browsing history when you exit the program. Check your browser's support site for details on how to maximize the program's security settings.

But no amount of technology can replace our human ability to spot something fishy. When in doubt, don't click. These days, sometimes you don't even need to *click* to be infected. Simply visiting the wrong page at the wrong time can infect your computer. Legitimate sites can be infected by malware-laced ads, which is why it's so important to maintain your computer's antiviral defenses. Don't forget antivirus for your tablet and phone, too: Viruses can strike any device, any time.

The computer you use for research should have all system and app updates installed. If you have an old Windows XP or Vista computer, or an older Mac, your risks increase. These systems can't be protected from modern threats, so use them with caution. Never access your financial accounts from an older computer if you can help it.

Lastly, keep a clean offline backup of your data. If you become infected by some of the nastier computer viruses, that backup may mean the difference between preserving your manuscripts or losing them forever. Grab a spare hard drive and copy those files, test to make sure you can recover them, and then store the drive somewhere safe.

I urge you: Why not take a few moments to assess your internet safety strategy now? To protect both your writing and your professional reputation, it's well worth the time and effort. W

Triona Guidry is a freelance writer and computer specialist based in Chicago.