Staying Safe and Secure Online

By Robert Trinchet

ROBERT TRINCHET

Robert, LNWM's director of technology, has more than a decade of experience in both financial services and IT.

How much more are you using your electronic devices? Chance are a lot more since the outbreak of Covid-19. A quiet revolution is taking place as many of us are relying primarily on digital devices to work from home, shop, socialize, exercise, and relax. The ramp up in online activity means more opportunities for bad actors to gain access to your digital devices and info. And so I thought I would summarize the latest best practices for protecting yourself digitally, in order of priority, as well as what we are doing at LNWM to keep your data safe and secure.

#1. Back up your data. The word "data" sounds bland and does not convey the priceless information many of us have on our laptops, desktops, cell phone and other devices. From tax forms to baby photos, losing this data can be devastating. This is why data backup is the #1 item on my list, given all that can go wrong in the physical world (fires, burglary, malfunction, etc.) and the rising threat of ransomware. With technology, you can never go forward if you can't go back.

Solution: The best practice is a layered approach: (1) An external hard drive on your desk (costs anywhere from $50 to $200) that is large enough to back up the files on your devices (desktop, laptop, phone). You should opt to encrypt this external drive to keep it secure. Note that Windows, Mac iPhone, and Android devices all have built-in backup apps that are largely automatic.

(2) An online service that stores your data remotely (in the cloud), encrypted and in real time, and which keeps that data private, since it can only be accessed through a password/encryption key issued to you. There are quite a few companies now offering data backup for individuals for relatively modest fees, including Backblaze, OneDrive, and iCloud. Just make sure your backup service supports full encryption.

If something happens to your external hard drive, you have encrypted backups in the cloud. And if something happens to your cloud access, you have your extra hard drive handy.

#2. Access the Internet privately and securely. The wi-fi you use to access the Internet at your house is relatively secure because it should be password-protected – but it is not private. Several years ago, the US government ruled that Internet Service Providers, such as Comcast and CenturyLink, can track your online activity without first obtaining permission. Also, if you venture out of your house to public spaces (airports, hotels, etc.) the free wi-fi there is suspect, not secure and not private.

Solution: Get encrypted access to the Internet anywhere (home or in public) through a Virtual Private Network (VPN). There are many free VPNs, but they are not recommended; their revenue model is based on free tools, so they can track you online and then sell your online habits to advertisers or other businesses. Reputable VPNs, such as of EasyVPN, mullvad.net, and TunnelBear (now owned by McAfee) charge a monthly fee and are publicly audited to ensure they do not scan or keep any logs of your activity. The websites you visit through a reputable VPN hide and encrypt your online activity.

You might also want to consider adding a dedicated "firewall," a device that sits between your home network and your Internet Service Provider, offered by companies such as Cisco, Fortinet or Ubiquiti. The most common type of firewall now is referred to as UTM (Unified Threat Management) and usually requires the know-how of a network specialist to set up. A UTM firewall not only blocks unwanted network traffic and dangerous websites, but it scans all traffic for viruses and malware.

STAY-SAFE PRACTICES

- TREAT EMAIL WITH SUSPICION. Hackers have gotten very, very good at sending emails that look legitimate, as if they're from a friend, relative or trusted institution. This is why all email is now suspicious, especially if the email contains a link and/or attachment.
- DO NOT AUTOMATICALLY CLICK ON EMAIL LINKS OR DOWNLOAD ATTACHMENTS. Both of these "add-ons" are common ways to get at your device. Clicking on a malicious link doesn't set off alarm bells. You may think: "Oh, that's just an error message," or "wrong website." What may not be apparent is that the website you were on for less than a second in installing ransomware as you type or is capturing your browser data as you surf the web, including any passwords or log-in information stored on your browser! When in doubt, delete the email and always go directly to the website rather than clicking a link.
- "HOVER TO DISCOVER" MALICIOUS LINKS. If you get an email that includes a link, ALWAYS hover over the link. If you do that, the website address for the link will appear, usually near the link or on the left bottom of your screen. If you do not recognize the web address shown, or if it seems suspicious to you, do NOT click on the link and delete the email.
- USE "MULTI-FACTOR AUTHENTICATION" OR MFA. LNWM's client portal and many other websites now allow for a two-step sign-in process. In addition to providing a password, you are asked to confirm your identity each time you log in by answering a personal question or a randomly generated number that is texted to your phone or sent to your email. MFA is much harder to hack, and we encourage our clients to add this feature not only for the LNWM portal but on all important websites they use.
- BE WARY OF "FREE PUBLIC WI-FI." Before logging in via a public network at a hotel, airport or coffee shop, STOP to think: Am I working on something that is OK for everyone around me to see? While traveling, you might want to bring a device just for Internet access, with no sensitive information on it. Or pay to use a Virtual Private Network (VPN).
- PROTECT YOUR ELECTRONIC DEVICES. The software on devices sold after 2010 should be set to automatically update itself. All you need to do is (1) update your anti-virus by buying the latest version; (2) do not change the default settings for your computer's firewall and for its automatic updating. It's also safer to turn your computer off when you're not using it and to periodically change the password for your home Wi-Fi network.
- BEWARE OF BOGUS COVID-19 WEBSITES. Thousands of new malicious websites offer COVID-19 remedies, treatments, cures, testing but what they want is your personal information. Best to go to reliable sites like CDC or UW Medicine for advice on the virus and treatments.

#3. Know the new rule on passwords. The new best practice for passwords, especially for important sites you visit often, is 25 characters. That is a lot. The good news is that those 25 characters can be all letters, preferably four different words that make no sense to anyone, but have special meaning for you. And once you set the password of that length, there is rarely a need to change it. Why? Because research shows that it can take an average of 100 years for a computerized system to crack a long, multi word password.

How do you keep track of various really long passwords? A good option (and one I suggest) is to install a password manager app on your phone or your computer that you access through a single, strong 25-character password unique to you. These apps, offered by companies such as 1Password or Dashlane, should reside "locally" on your devices, and not in the cloud. Although most companies offer synced, encrypted password storage in the cloud, I prefer keeping passwords secured on a local protected device.

WHAT LNWM IS DOING

How do we go about keeping your personal information private and secure at LNWM? While we use specific strategies and tools that we do not make known, overall we have a three-pronged approach: (1) layers of security; (2) ongoing employee training; and (3) constant vigilance.

Layers of Security: The basis of most security strategies, including ours, is layering. You can think of the various security measures that we use the same way you think about safeguarding a house:

- **Internet-based security tools** – These are the equivalent of tall fences and security guards on the outside, working to keep hackers from ever reaching the LNWM network.
- **Network "firewalls"** – these are like dead bolts on all of LNWM's external network doors to keep hackers out.
- **Internal network monitoring** – our alarm system in place in case of break-in.
- **Controls on access to information** – the equivalent of a hard-to-access safe.
- **Data loss prevention** – to monitor and block information leaving our network to ensure it does not contain your personal information – like a security guard.
- **Tracking and logging of network activity** – akin to security cameras, helping us identify who is doing what inside and around the LNWM network.

Employee Training: Despite all the layers of security, all networks (including ours) remain vulnerable to an employee unintentionally opening the door to the equivalent of a smooth-talking conman. Hackers call this "spear phishing," and it usually starts with a message to employees' work emails, tempting them to click on a link or open a file. If anyone falls for the bait, presto! The hacker can potentially break through a layer of security.

Fighting phishing requires ongoing vigilance by everyone. This is why all LNWM employees are trained to look out for suspicious emails, especially ones that make a financial request or have links

and attachments. We have annual security training, random testing to keep awareness up, plus periodic data security briefings. What if an employee is duped by hackers? We have in place strong containment measures: the equivalent of the alarm system, safe, and security cameras described earlier.

Constant Vigilance: To protect against new threats, we get alerts about newly discovered vulnerabilities and update our systems accordingly.

What about the cloud? Most major businesses, including LNWM, now use web-based services, aka "cloud computing." This is just a catchy name for data storage and processing on computers that someone else owns. By closely monitoring our cloud providers and using the latest security protocols to access the cloud we're able to mitigate the risks. Also, since cloud computing has become commonplace (Seattle's Amazon.com and Microsoft are two of the biggest cloud-service providers), the IT industry is devoting huge resources to address cloud safety and security issues and we adhere to the best guidance.

IF YOU DO GET HACKED

1. CLOSE THAT EMAIL ACCOUNT

If you can, immediately close the hacked email account. If you need to keep that email address, change the password immediately to a strong password using a computer that hasn't been compromised.

2. UPDATE YOUR FINANCIAL ACCOUNT ACCESS

Go to another computer and change the passwords on all your financial accounts. If they offer Multi Factor Authentication, activate it. Consider asking the three major credit bureaus to add an "Initial Fraud Alert" to your credit record. This would require extra identity verification for 90 days, in case someone tries to apply for loans or credit cards under your name.

3. CLEAN THE COMPROMISED COMPUTER

Take your machine to a service center, such as Best Buy's Geek Squad, to be scanned for viruses. Even better, have the hard drive wiped clean and the software reinstalled (remember backup rule #1?). If you're using a cloud service like Microsoft's Office 365 or Apple's iCloud, pictures and email should already be saved online so you won't lose important records.

4. CHECK YOUR EMAIL SETTINGS

Look for unexpected "Rules" and "Forward" settings on your email account. Hackers often set up rules to forward emails from financial institutions to email accounts they control.

5. NOTIFY YOUR CONTACTS

Tell the people on your contact list that your computer was compromised. Hackers often try to scam your contacts.

ABOUT THE AUTHOR

Robert Trinchet is director of technology at Laird Norton Wealth Management (LNWM). He and his team implement IT solutions that keep LNWM client information secure and enhance account management, analysis and reporting. Robert has more than a decade of experience in IT and financial services. Prior to joining LNWM, Robert served as VP of Private Wealth Technology Operations at SunTrust and as the Chief Information Officer at GenSpring Family Offices. Before that, he held technology leadership roles at Kaiser Permanente, Cigna Health, and the Chicago Tribune.

ABOUT LAIRD NORTON WEALTH MANAGEMENT

With more than $5 billion in assets under advisement, Laird Norton Wealth Management is the Northwest's premier wealth management company. Founded in 1967 to serve the financial management needs of the Laird and Norton families, the firm now provides integrated wealth management solutions to more than 600 individuals, families, business leaders, private foundations and nonprofit organizations.

801 Second Avenue, Suite 1600, Seattle WA 98104 206.464.5100 800.426.5105 lairdnortonwm.com

DISCLOSURE