8 Tips To Keep Your E-Data Safe

By Bill Frizzell

BILL FRIZZELL

is Laird Norton Wealth Management's Director of Technology since 2005, has many years of experience in both international banking and IT. His focus is on delivering secure, best-in-class systems for clients and LNWM's internal operations.

Recent hacker attacks on Equifax, Yahoo, Whole Foods and even the IRS make it clear: It's a challenge to keep your data private and secure in the Internet age. While there's no way to be absolutely safe, there are things you can do to protect yourself from someone trying to hack your electronic devices. Let's discuss that first. Then I'll describe what we're doing at LNWM to keep your personal information safe and secure.

What You Can Do

- **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 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 goes on to quietly capture your browser data as you surf the web, including any passwords or log-in information stored on your browser!
- **"Hover to Discover" malicious links.** If you get an email that includes a link, ALWAYS hover over the link with your mouse. 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.
- **Put some effort into creating strong passwords.** If not, you're making it much easier for hackers to figure out your password and gain remote access to your computer and browsing history. Consider this: Internet-security experts estimate that adding just 1 capital letter and 1 asterisk to an 8-character password could increase the time required to figure out the password to a daunting 14 years, from a quick 52 seconds!

  A strong password has a mix of upper and lower case letters, numbers and punctuation. It should be at least 8 characters long and preferably 10 or 12. Be sure you don't use names, birthdates or just one word that can be found in dictionaries.
- **Vary your passwords.** If hackers access any one of your passwords, they rush to try it on all major financial websites to see if one of your accounts turn up. It's especially important that the password for your main email account is different from your online financial accounts.

Laird Norton Wealth Management

801 Second Avenue
Suite 1600
Seattle, WA 98104

www.lairdnortonwm.com
206.464.5100 | 800.426.5105

- **Start using "multi-factor authentication."** 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. Multi-factor authentication 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.
- **Protect your electronic devices.** If you bought your device after 2010, the software should 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.

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 using a computer that hasn't been compromised.

2. Update financial account access

Go to a safe machine and change the passwords on all your financial accounts. 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. 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.

What LNWM is Doing

How do we go about keeping your personal information private and secure at LNWM? We use 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.
  - **Tracking and logging of network activity** – akin to security cameras, helping us identify who is doing what inside the LNWM network.

- **Employee Training:** Despite all the layers of security, 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 waltz in through the network's back door.

  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 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.

ABOUT LAIRD NORTON WEALTH MANAGEMENT

With nearly $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.

DISCLOSURE

All investments involve a level of risk, and past performance is not a guarantee of future investment results. The value of investments and the income derived from them can go down as well as up. Future returns are not guaranteed and a loss of principal may occur. All investment performance can be affected by general economic conditions and the extent and timing of investor participation in both the equity and fixed income markets. Fees charged by LNWM will reduce the net performance of the investment portfolio.

The information presented herein does not constitute and should not be construed as legal advice or as an offer to buy or sell any investment product or service. Any opinions or investment planning solutions herein described may not be suitable for all investors nor apply to all situations. All opinions expressed are those of Laird Norton Wealth Management and are current only as of the date appearing on this material.

Any accounting, business or tax advice contained in this presentation (or communication, including attachments and enclosures) is not intended as a thorough, in-depth analysis of specific issues, nor a substitute for a formal opinion, nor is it sufficient to avoid tax-related penalties.

Some investments may not be publicly traded and they may only allow redemptions at certain times conditioned on various notice provisions and other factors as more fully described in the related offering and subscription documents provided at the time of the investment. Due to the nature of these types of investment funds, hedge funds, fund of funds, and similar partnership-like investment vehicles, they should be considered illiquid. In addition to restrictions on redemption, they often include holdback provisions that may delay a full redemption for several months or longer. There is no guarantee that the amount of the initial investment can be received upon redemption. Due to the nature of the tax reporting that may be available from these types of investments, clients should expect to extend the filing of their tax returns.

A benchmark is an unmanaged index, and its performance does not include any advisory fees, transaction costs or other charges that may be incurred in connection with your investments. Indices are statistical composites and are shown for informational purposes only. It is not possible to invest directly in an index. Indices are unmanaged and are not subject to management fees. Any benchmark whose return is shown for comparison purposes may include different holdings, a different number of holdings, and a different degree of investment in individual securities, industries or economic sectors than the investments and/or investment accounts to which it is compared. Comparisons of individual account or portfolio performance to an index or benchmark composed of indices are unreliable as indicators of future performance of an actual account or portfolio. Actual performance presented represents past performance net of investment management fees unless otherwise noted. Other fees, such as custodial fees or transaction related fees may not be reflected in the actual performance results shown.

Certain information herein has been obtained from public third party data sources, outside funds and investment managers. Although we believe this information to be reliable, no representation or warranty, expressed or implied, is made, and no liability is accepted by Laird Norton Wealth Management or any of its officers, agents or affiliates as to the accuracy, completeness or correctness of the information herein contained. In addition, due to the nature of an investment or the date of the creation of the attached presentation, some values shown or used in the calculation of performance may be based on estimates that are subject to change.

The attached materials may contain confidential information that is intended only for the person to whom it is presented. By accepting this information, you agree to maintain its confidentiality and not to distribute it to any other person without the express permission of Laird Norton Wealth Management. All data presented is current only as of the date thereon shown. Laird Norton Wealth Management is comprised of two distinct entities that may offer similar services to clients. Laird Norton Trust Company is a State of Washington chartered trust company. Its wholly owned subsidiary, Laird Norton Tyee Asset Strategies, LLC, is an Investment Advisor registered with the Securities and Exchange Commission. Such registration does not imply any level of skill or expertise.