ViewPoints

Cybersecurity – Protecting Your Information

Entasis

ASSET MANAGEMENT

Last year, there were over 14 million victims of identity theft and fraud.

It might sound a bit dramatic, but every day there are criminals around the world that conspire to steal your username and password, obtain your Social Security number, open credit cards in your name, seize your computer and drain your bank accounts.

Most people don't realize how vulnerable they are or what they can do to maximize their security. As your investment advisors, we believe it is important to share some best practices to help you out. In this document we want to share 10 RULES you can put in place to better secure your information.

1) Create a Secret Email Address for Your Financial Accounts.

Our email address is the key to our digital lives. We share it with countless businesses, organizations, and people. If you've used the Internet for any amount of time, you have entered your email address at a host of online accounts for shopping, traveling, exercising, gaming, dating, and more. We don't think twice. But having your email addresses in so many databases puts you at a significant risk. Hackers routinely breach the security networks of many organizations that hold your primary email address. That stolen personal data, paired with poor email security, leads to disaster. A separate email address reduces your digital footprint and if your primary, non-financial email address is exposed in a hack, it will not be connected to your financial accounts.

2) Create Strong Passwords.

Many passwords we use are child's play for hackers. Computer power gets stronger with each passing year. That means the bad guys can figure out your password in no time flat. Did you know that it only takes 17 minutes for a computer to crack 1,000 weak passwords? One reason for this is that people choose passwords that have less than six characters or they use names, dictionary words, or other common passwords like "password" or "123456." Three suggestions to improving passwords are to build passwords using a mnemonic or a goal. In each instance because the passwords are difficult to remember you should consider a password manager or offline storage.

- Mnemonic example – Jack and Jill went up the hill could be J&Jw^thH!ll
- Goal setting example – Run everyday could be Run3v3ryd@Y

3) Enable 2-Step Verification on Your Email and Financial Accounts.

This extra layer is a relatively new trend in online security called two-step verification or sometimes two-factor authentication. It should be added to any account you have that supports the technology. With this approach, when you start to log in to an account online, you're sent a short-lived, one-time passcode. You must use that code to finish logging in. You can receive this code via text message, or something called an Authenticator App. The Authenticator App is the most secure option as it is more difficult for hackers to compromise. Some popular Authenticator Apps are Google Authenticator and Microsoft Authenticator. This method stops your accounts from getting hacked because it requires two separate things: something you know, your password, and something you have, the temporary code. So even if a hacker has your password, he won't gain access, and you'll be alerted if someone is trying to break into your account.

4) Use Wi-Fi with Extreme Caution.

We all love free Internet access when we are out and about and want to be connected. But that free connection can end up being very costly. These free networks are completely open, and hackers can gain access to anything you do while connected—your email, your credit card number, your bank account—you see the pattern here. It could be very bad. When connected to free, public Wi-Fi, avoid making financial transactions or checking your email. Instead, you can use your smartphone as a hot spot for your computer. When you do, you'll be using your data which provides a private connection rather than the public wireless network. If you need to connect regularly on–the-go, a VPN (Virtual Private Network) would be a good option. This device allows you to create your own private Wi-Fi network anywhere you go.

5) Secure Your Home Wi-Fi Network.

These are some of the more technical actions you'll have to take. Don't be discouraged if it sounds difficult to you. If you are confused, I advise you to contact the tech-person in your life for help. To do these steps, you'll have to log in to your router's IP address. If you do not know your router's IP address, you can find it in your user manual or by searching the make and model of your router online.

- Change the default username and password. Hackers know these and will use them to try to break into your network. Pick a strong password.
- Encrypt your router. Be sure to select the strongest encryption setting for your router-WPA2 or WPA3. WEP is no longer considered secure, and you should replace your router if your only option is WEP.
- Disable Wi-Fi Protected Setup (WPS). This feature allows others to quickly connect to your network with a short passcode rather than having to type the whole password. But it can lead to strangers gaining access. If you don't have the option to fully disable this feature, see if you can limit the number of attempts a person can make to log in.
- Update your router firmware (a fancy word for software). The majority of routers come with outdated software which leaves your network vulnerable to attacks. Updating your firmware sounds like a daunting task but it's not that bad. Follow the instructions in your user manual for detailed instructions.

6) Get Instant Text or Email Alerts from Your Credit Cards and Bank Accounts

Every time a charge is made to one of your financial accounts your bank instantly knows. Why shouldn't you? Setting up alert notifications for all charges or withdrawals is simple. Most changes can be done online. Contact your bank or credit card company for help.

7) Freeze Your Credit and Protect Your Children

By default, our credit files are open. That means anyone with enough information to impersonate you may be able to open a new line of credit in your name. It happens all the time and is a major source of identity theft. And when you consider how many private and public organizations have been hacked—institutions we've trusted with our SSNs, employment history, and other details about our financial lives—you need to be worried about the state of your credit file at the big three agencies.

A credit freeze locks your credit file with a PIN at each of the credit bureaus. No new credit can be issued in your name unless you lift the freeze with your special PIN. You will have to contact each of the credit bureaus separately. Credit freezes are free in every state thanks to a federal law passed in 2018. A credit freeze puts you in control. It is way more secure than credit monitoring or a fraud alert, both of which will alert you after credit has been issued in your name. With a credit freeze, you can prevent identity theft from happening instead of cleaning up after your identity theft nightmare. But if you have children, it isn't just your credit you should worry about….experts estimate that 500,000 children suffer from identity theft each year because parent or guardians don't think to check. Make sure to go through the same process for children as well.

8) Update Your Software.

It is estimated that 40% of computers don't update their software in a timely fashion. And security experts say 75 to 80% of the computer hacks they see relate to outdated software. Hackers exploit security holes in unpatched software which allows them to install malware and viruses on your unprotected devices. This malware could record everything you do or kidnap your computer for ransom. So, you want to be sure that all the software and programs on your devices are up to date. That includes your operating system, your browsers, Microsoft Office, Adobe programs, and more.

9) Back Up Your Files to Avoid Ransomware Extortion

One type of malware that is a huge threat today is ransomware. In this attack, hackers infect your device with malware that encrypts everything on your computer—you can no longer access any of your files. In order to get your files back, you must pay the hackers a bitcoin ransom. In order to avoid paying ransom to cyber crooks, you need to follow the "Rule of Three" meaning you need to back up all your files in data in three different places. The first is on your computer or device. Next, you need to save a copy of your files and data to a physical backup device—something like an external hard drive. Lastly, you need to save your data to a cloud service like Dropbox, iCloud, or OneDrive.

10) Take Time to Examine Email Messages and Inspect Links

Most email scams start out with an urgent action request. This should be an initial alert to you. Second, take time to determine the true sender of an email. Many scams can fake the sender. Use your mouse to hover over the display name. A small box will appear with the true email. Third, never click on an unsolicited attachment. It could be a .exe file that plants a virus. Finally, be aware of poor grammar, emails that don't use your real name and a vague signature line. If it feels suspicious it probably is.

We know this can feel daunting. It is unfortunate there are so many scams out there. But we believe these 10 rules can go a long way to keeping your information safe. Thank you for taking the time to read it. If you have questions about any of these points, please reach out to us.

Our Team

Bob Batchelor, CFA®, CFP® is Co-Founder and Chief Executive Officer of Entasis Asset Management. Bob has 25 years of experience in the investment industry. Prior to founding Entasis, Bob worked at Artisan Partners where he held a variety of roles including Head of Corporate Communications, Managing Director, Head of Marketing and Technology and Head of Marketing and Communications. He also served as a member of Artisan Partners Executive Committee. Before Artisan Partners, Bob worked at Strong Capital Management as Client Account Manager and Director of Investment Research and Communication.

Bob holds an M.B.A. from Marquette University and a B.B.A. from the University of Wisconsin-Madison. He has earned the right to use the CFA designation. Bob is a member of the CFA Institute and CFA Society of Milwaukee. Bob has also earned the right to use the Certified Financial Planner™ certification and SE-AWMA™ professional designation.

Charles (C.J.) Batchelor, CFA® is Co-Founder and Chief Investment Officer – Equity of Entasis Asset Management. C.J. has 19 years of experience in the investment industry. Prior to founding Entasis, C.J. worked at Cleary Gull, a multi-billion dollar investment advisory firm, as Director of Investment Research. He also served as a voting member of Cleary Gull's Investment Policy Committee, Investment Committee and Equity Strategy Group.

C.J. holds a B.B.A. in Finance from the University of Wisconsin-Milwaukee. He has earned the right to use the CFA designation. C.J. is a member of the CFA Institute and CFA Society of Milwaukee.

Mike Peters, CFA® is Co-Founder and Chief Investment Officer – Fixed Income of Entasis Asset Management. Mike has 19 years of experience in the investment industry. Prior to founding Entasis, Mike worked at Cleary Gull, a multi-billion dollar investment advisory firm, as Fixed Income Portfolio Manager. In his role he served as a voting member of Cleary Gull's Fixed Income Strategy Group and Complement (Alternative) Strategy Group. Before Cleary Gull, Mike worked for several years at Madison Investment Advisors, a multi-billion dollar asset management firm, as a Fixed Income Analyst.

Mike holds a B.B.A. in Finance from the University of Wisconsin-Milwaukee. He has earned the right to use the CFA designation. Mike is a member of the CFA Institute and CFA Society of Milwaukee.

David LaCroix is a Senior Financial Advisor at Entasis Asset Management. David has more than 50 years of experience in the investment industry. Prior to joining Entasis, David worked at Cleary Gull Advisors, a Johnson Financial Group Company, and Cleary Gull Inc., a prior affiliate of Cleary Gull Advisors, where he most recently served as Vice President, Relationship Manager responsible for high net worth clients. Before Cleary Gull, David worked in a variety of portfolio management and client relationship management positions with A.G. Edwards and M&I Capital Markets Group.

David received his M.B.A. and B.B.A. in Finance from the University of Wisconsin-Madison. He has served as a member of the Archdiocese of Milwaukee Investment Committee, as a Trustee for the Village of Shorewood and as Director/Treasurer of Milwaukee Summerfest.

Entasis Asset Management
262-754-5299
Info@EntasisAM.com

FOLLOW US

IMPORTANT INFORMATION

Statements may be forward looking and are not intended as specific investment advice without further review of individual circumstances. Commentary, opinions, analysis, and recommendations may be subjective, do not guarantee future performance, and could change at any time without notice. Under no circumstances does the information contained within represent a recommendation to buy or sell any security. Charts and graphs are provided for illustrative purposes only.

This information is provided for informational purposes only and does not constitute individualized financial advice or create an advisor-client relationship. An advisor-client relationship is only created by the execution of a management agreement by us and the individual or entity to whom we provide individualized services.

Information contained herein is as of the date hereof unless otherwise noted. Entasis is under no obligation to update such material or information.

Sources:
https://www.savvycybersecurity.com/default.aspx