BY Andy Park
Wealth Advisor

Cybersecurity: Starting the Conversation

Technological growth over the last half-century has been nothing short of astounding. Take, for instance, the mobile phone. When it was first developed in 1973, it was as hefty as a brick and only allowed for 20 minutes of talk time before you had to wait 10 hours for it to fully recharge.[1] Fast-forward a few decades and now, thanks to advances in mobile technology and the advent of the internet, you can use your phone to check email, see who's at your front door, deposit checks, start your coffee maker or your car, and film your loved ones celebrating their birthdays.

These advancements are certainly convenient, but they've also provided more ways for cybercriminals to intrude on our lives. According to the FTC, there were 1.1 million reports of cyberfraud in 2017, with approximately $905 million in total losses. That's up from only $63 million of total losses in 2016.[2]

We must be as determined to protect our personal information as cybercriminals are to access it. And, as stewards of your wealth, protecting your assets is part of our job. That's why we're talking to clients more and more about the importance of practicing good cybersecurity and what they can do to help protect themselves. This article highlights common best practices and key tips we provide to our clients. It represents the start of what will certainly be an ongoing conversation in the years ahead.

Going Phishing

The most common cyberthreat is some form of phishing attack. Like its namesake, a phishing attack attempts to lure its victim by pretending to be something that it's not. Phishing is any attempt to trick victims into sharing sensitive information. We've all seen and heard of those emails promising us a large cash prize if we simply supply our bank account information and Social Security number. Or the so-called Nigerian Prince scam, where, for a mere $10,000, a jailed prince promises to send you $100,000 in the next 10 days. These emails, littered with typos and strange syntax, are usually sent to the masses in hopes that someone will be naive enough to take the bait.

A Cybersecurity Glossary

Phishing
Sending fraudulent, generic emails in the attempt to lure victims into sharing sensitive information.

Spearphishing
Making more sophisticated, targeted phishing attempts, with emails personalized to the target, sometimes leveraging information found on social media.

Whaling
Spearphishing high-profile and high-net-worth individuals, generally based on in-depth research of targets' online profiles and publicly available information.

Spoofing
Impersonating an individual in an attempt to convince others to reveal sensitive data.

Malware
Malicious software that impairs your computer/device or allows attackers to gain access to it.

In more sophisticated attempts, cybercriminals target certain individuals based on information gathered by scouring social media sites like Facebook, Instagram, and »

LinkedIn. Two examples of this type of targeted phishing are spearphishing and whaling. As opposed to phishing, spearphishing is targeted to a specific individual. So instead of the generic "Dear Sir," the spearphishing email reads, "Dear Andy." Whaling takes spearphishing a step further by targeting high-profile (presumably high-net-worth) individuals like C-level executives, politicians, and celebrities. Targeted phishing attacks typically include instructions to take immediate action (click on a link, call a phone number, or download a file). This action may make it easier for your attacker to get your sensitive information (either from you or a third party) or to install malware, malicious software that allows the attacker to gain access to your computer or device.

Another common attack is spoofing. Spoofing occurs when an attacker impersonates you to convince others to send or reveal your sensitive data. For example, an attacker might email your accountant from an email that *looks* like yours with a request to send your latest tax returns. These attacks—phishing and spoofing—usually go hand in hand. Once hackers gain access to your email or personal information by phishing, they can more readily engage in spoofing, potentially ensnaring more unsuspecting victims by impersonating you.

Cybersecurity Health

Just like disease, cyberattacks can spread easily and adapt to the medicines made to fight them off. And, just as living a healthy lifestyle requires dedication, discipline, and continual learning, maintaining healthy cybersecurity habits requires time, effort, and agility. The key is to scrutinize anything that seems out of place. "You can never be too careful" is a great cybersecurity motto.

When you receive a phone call from a distant relative you've never even heard of, question it. When you receive an email you weren't expecting with links you're being asked to click on, question it. Hover the mouse over the link to see if it's directing you to a website you know and trust. And confirm the identity of the email sender by verifying the contact information in the email and comparing it to the company's website or your contact directory. Making a phone call to confirm an email might seem like a tedious extra step, but it never hurts to be cautious.

Healthy Technology Habits

Keep your operating system, web browsers, and antivirus systems up to date. Doing so ensures that when software vulnerabilities are caught and fixed, you receive the latest patches and are protected.

Set unique passwords for all accounts so that, if one password is compromised, an attacker won't have access to all of your accounts.

Change your passwords regularly and don't share them with anyone else.

Consider a password manager like Last Pass or Dashlane if managing passwords becomes too burdensome. These managers help you securely store all your passwords in one place.

Working Together

The relationship you have with your advisor and support team is instrumental in preventing cyberattacks. The more you know each other—voice, habits, turns of phrase—the easier it is to recognize a spoofed email or phishing attempt. Similarly, being familiar with the formatting of RMB emails, links, and webpages can help you identify communications that are out of the norm.

Expect to have more conversations with your advisor on the topic of cybersecurity—we are here to discuss any questions or concerns you may have. By working together and remaining vigilant, we can maintain cybersecurity health and strengthen our resistance to cyberattacks. ■

1 *Suzanne Deffree, "1st mobile call is made, April 3, 1973," EDN Network, April 3, 2019, https://www.edn.com/electronics-blogs/edn-moments/4411258/1st-mobile-phone-call-is-made--April-3--1973.*

2 *"Consumer Sentinel Network Data Book 2017: Executive Summary," Federal Trade Commission, accessed May 3, 2019, https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/executive-summary.*