Key Questions

May 23, 2022

How Can You Protect Yourself From Cybersecurity Threats?

Nancy L. Anderson, CFP®, Regional Planning Strategist, Key Private Bank

Tammy Gedetsis, Senior Manager, Information Security, KeyBank

The Key Wealth Institute is a team of highly experienced professionals from across wealth management, dedicated to delivering commentary and financial advice. From strategies to manage your wealth to the latest political and industry news, the Key Wealth Institute provides proactive insights to help grow your wealth.

In recent years, we have witnessed a swift transformation as more and more of our finances have been brought online. Growth in digital banking accelerated during the COVID-19 lockdowns out of necessity—and with this added convenience comes a new set of challenges related to cybersecurity risk. With more at stake, criminals are becoming more and more sophisticated in their approach to accessing our information.

The ongoing war in Eastern Europe has also raised a new set of questions regarding the influence of state-actors in cyberattacks, and whether we should be thinking about risk and our personal data security differently.

Understanding Motivation

The most important psychological principle of cybercrime is human engineering, or the idea that criminals prey on fear and basic human empathy to elicit an emotional response to get us to act. Therefore, many criminals impersonate charities requesting donations, or a colleague requesting a favor – people are generally less skeptical of organizations claiming to do good and are more willing to go out of their way for a person of authority.

This background helps explain why phishing is the most prevalent form of social engineering that allows ransomware to encrypt files on a device and render systems unusable. The risk is minimal, and the reward can be immense if the right person clicks through to a malicious link, opens a corrupted file or discloses some key component of their personal information. A ransomware attack of this kind is particularly detrimental because one employee could theoretically open their entire corporate network to the attacker. This was the case when Colonial Pipeline in the Southeastern United States fell victim to a ransomware attack last year when the criminals were able to access their network by stealing one password. What this tells us is to always stop before clicking a link to ask yourself, “Is this request in line with what this person has asked of me in the past?”

Despite Russia’s invasion and the threats made against the West, data from February shows that nearly three-quarters (73%) of current security events are related to cybercrime, compared to the 7% of events related to cyber warfare.

During this period, there were 16 events targeting finance and insurance, and only one was an act of warfare. All this to say, financially motivated crime is still the most prevalent driver of cyberattacks – and the steps needed to defend against them are consistent, irrespective of whether the attack is financially or politically motivated.

How Can You Protect Yourself From Cybersecurity Threats?

Cybersecurity Checklist

The uncertainty of the past few years has taught us the importance of taking precautions and prioritizing preparedness, and the same outlook should be applied to cybersecurity. We recommend taking the following steps to limit the likelihood of falling victim to an attack:

- Strengthen Passwords – It goes without saying that using the same password across many accounts would create a major security risk if criminals were to get ahold of it. In addition to employing unique passwords, using longer passphrases is even better. Sequences longer than 15 characters, with very specific words, characters and spaces make it significantly more challenging for criminals to guess. For help managing different passwords/ passphrases, you can use a password manager.

- Set-Up Multifactor Authentication – You've likely experienced using multifactor authentication to access your company's network, but it is equally important for protecting your personal accounts. Setting it up requires you to provide two or more verification factors to access an account – this includes something you know (i.e. password), things you have in your possession (i.e. smartphone), or a personal signifying feature (i.e. fingerprint biometrics). The latter two factors present a much greater challenge to criminals, even if they happen to have your password on hand.

- Update Your Software – While it sounds simple, updating your computer software as security patches are rolled out is a very easy but important way to prevent cyberthreats. When software updates are pushed through, the details about software vulnerabilities are typically disclosed, and criminals can leverage these identified weaknesses to target victims that may not have updated their software yet.

- Connect to the Internet Safely – While you shouldn't second-guess connecting to your home internet, accessing the web from public Wi-Fi networks in parks, airports and cafes can present a security risk, as it would be difficult to verify how secure the connection is. If possible, avoid using these networks, especially if what you need to do involves accessing sensitive information like checking a bank account.

- Leverage Security Tools – Many tools have been developed in recent years to assist in prioritizing cybersecurity as more and more important information is held online. Browser reputation tools like Web of Trust, for example, are plug-ins that alert you to the expected safety of each website that populates in a browser search. Likewise, alternative browsers like Mozilla Firefox and Brave Browser have less exposed security vulnerabilities than more commonly used browsers like Google Chrome and can promote privacy by limiting data mining.

As digital finance continues to evolve and new technologies emerge to simplify our financial lives, practicing regular cybersecurity "hygiene" to protect our information and assets will ensure bad actors won't succeed. For more information and insights from experts across our cybersecurity, technology, and banking solutions teams visit Key.com/cybersecurity.

To learn about additional strategies to protect your data, please contact your advisor.

About the Authors

As a Regional Planning Strategist for Key Private Bank, Nancy Anderson proactively advises clients on the development of a personalized, comprehensive financial plan that creates a financial roadmap so they can make more informed, confident decisions.

A nationally recognized expert in retirement planning, Nancy has penned a popular personal finance column on Forbes.com since 2012. She has also provided guidance and advice to high net worth clients since 2001. Nancy is a CERTIFIED FINANCIAL PLANNER™ (CFP®), and has a Bachelor's degree from the University of California, Davis. She is a member of United Way's Women United Organization and the Utah Financial Planning Association.

Tammy Gedetsis is a Senior Information Security Manager at KeyBank. She has been at KeyBank for 24 years focused on business clients and their digital experience. In her current role, she's responsible for the Cybersecurity Education & Awareness programs for all KeyBank employees, consumer and business clients. Prior to this role, Tammy was the Senior Digital Product Manager for Key's corporate digital platform, KeyNavigator where she was responsible for strategy and delivery of commercial products and services.

210714-1142677-1230623757