Securing Your Financial Accounts

Overview

Your financial accounts are a primary target for cyber-criminals. You have money, and they will do anything to steal it. By financial accounts, we mean not only your checking or savings accounts, but also investments, retirement, and online payment accounts like PayPal. Fortunately, with some simple, fundamental steps, you can protect yourself.

How they attack?

Banks invest a huge amount of money in securing their systems, making it extremely difficult for a cyber-criminal to hack into them. This is why cyber-criminals target you and your accounts instead. They know you don't have your own security team to protect you, so it's much easier to hack you than a bank. Here are the two most common ways they will target you and attempt to steal your money:

Passwords: Each of your financial accounts is protected by a password. If a cyber-criminal can guess or compromise any of those passwords, they can log in as you and then transfer your money to bank accounts that they control. There are numerous ways they will try to get your password. One common method is infecting your computer with malware. Once your computer is infected, they can capture your username and password when you access your bank's website. Another common method is sending phishing emails that pretend to come from your bank. When you click on the link in the email, you think you are logging into your bank's website, but in reality, you are logging into a fake website that the criminals control. This allows them to once again harvest your username and password, which they can then use to log in as you.

Asking: Cyber criminals can simply ask you for your password or for you to transfer the money to them. Such social engineering attacks often start by getting you on the phone. Cyber-criminals know that once they get you talking, it's much easier for them to use emotion to get you to make a mistake. This is why you are starting to see more phishing emails, voice mail, and browser pop-ups creating a sense of urgency by telling you that you have to call a phone number to resolve an issue or to take advantage of an amazing opportunity before it expires. Once you call the phone number, the criminals create a tremendous sense of pressure to either give them access to your accounts or to move your money to different accounts for them. For example, they may tell you they are from tech support or the government, claiming that your computer is infected and that if you don't act now, you will lose all your money.

Protecting Yourself

Fortunately, securing your bank accounts is simpler than you may think. Here are three simple steps to protect yourself.

Be Suspicious: First and foremost, you are your own best defense. If you get an email, text message, voicemail, or browser pop-up that seems odd or suspicious, it may be an attack. The greater the sense of urgency, and the more you are being pressured to act NOW, the more likely it is an attack.

Use Strong Passwords / MFA: Protect each of your financial and personal email accounts with a long, unique password. Can't remember all of those unique passwords? Consider using a password manager to securely remember and store them all for you. The best way to protect each of your financial accounts is to enable a feature called multi-factor authentication (MFA) on each account.

Monitor: Finally, monitor all your financial accounts. You can set up automated alerts that will email or text you any time money is moved into or out of your accounts. This way you can quickly detect any unauthorized or suspicious transaction. The sooner you detect something wrong and report it to your bank, the more likely you will be able to recover your money.

Guest Editor

Lynn Dohm is the Executive Director of Women in CyberSecurity (WiCyS). From her experience in the cybersecurity education sector to active involvement in grant-funded programs and nonprofits, Lynn advocates and spreads awareness on the importance of diversifying the cybersecurity workforce.
Twitter: @lynn_dohm. Linkedin: https://www.linkedin.com/in/lynndohm/.

Resources

Emotional Triggers: How Cyber Attackers Trick you: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Phishing Attacks Are Getting Trickier: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
Password Managers: https://www.sans.org/newsletters/ouch/password-managers/
Multi-Factor Authentication: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/