CERITY PARTNERS

Cybersecurity: Five Ways to Help Protect Yourself and Your Family

June 25, 2019

Stefan Ludlow, Director of Technology
Pierre duPont, Partner
Cerity Partners

Hardly a day goes by when there isn't press coverage of yet another password security breach, ransomware attack, or phishing attempt that comes right to our desks. What's a person to do?

Consider taking these five steps to help strengthen cybersecurity for yourself, your family and your small business, and to minimize the damage that may occur if you're hacked.

1. **Enable Two-Factor Authentication (2FA) for Your Online Accounts**
   Two-factor authentication offers an added layer of security. Whenever there is a login attempt on one of your online accounts, the service provider (your bank, for example) sends a message to your cellphone or "second device." This approach is generally more secure than a password alone because the hacker is unlikely to have your password and physically possess your cellphone at the same time. Before opening a new account, check to see if the business uses 2FA; the answer may influence your decision to use their services.

2. **Use a Password Manager and Don't Share Passwords**
   Take the time to get separate logins for your spouse, your children, your assistant at work, your accountant, whomever; any security professional will tell you sharing a password is nearly the worst thing you can do. It's generally not difficult to set up parallel and safe shared access if needed.

   Which leads to the next point: you, yourself, should not be using the same password on any two accounts—every place you log in should have its own unique and complex (lengthy) password. Using the same password on multiple sites is a common cybersecurity mistake many people make. Of course, it's difficult to generate and remember a long and complex password for multiple websites. That's where a password manager can come in handy. You can generally use them across all devices such as your cellphone, PC or Mac, and on most web browsers. Consider your choice carefully; make sure to read independent reviews of the different password managers or ask trusted individuals for recommendations.

3. **Live Wisely on Social Media**
   Lock down your social media sites so that only those friends or the "network" you have identified can see your information. Unless you are actively trying to become a social media influencer, there's really no reason to share your posts or feed publicly. And when you travel, don't post "live" on social media. Criminals can learn a lot about you and identify holes through which to attack you by looking at your social media profile.

4. **Be Cautious with Email**
   Personal information such as social security numbers, bank account numbers and passwords should not be sent via email unless you have a secure email system that encrypts the data before it leaves your computer or phone. Secure mail helps protect your private information in the event the email is inadvertently sent to the wrong party or possibly intercepted while in transit.

Also, hackers often use email to try and gain access to your computer. To protect yourself, only open attachments or click links you are expecting and are from a person or business you trust. Even if the message appears to be from someone you know, be sure to check the web address (URL) carefully; look for odd modifications such as the number "1" instead of the letter "l" or slight misspellings.

If you haven't already, create a backup system for your files and photos. You can do this yourself or ask a professional to set it up for you. Once established, your backup system will operate behind-the-scenes and may save you if you're hit with a ransomware attack.

5. Monitor Your Credit Report

If a business or service provider notifies you that your personal information was exposed during a security breach, monitor your credit report for any unusual activity (e.g., unauthorized accounts). And it's good practice to annually request and review a copy of your report from Experian, TransUnion and Equifax. As an added precaution, you can lock or freeze your credit with each of these agencies, although you'll need to remember to unlock it before making certain purchases like a car or home.

Many of these points may seem like common sense, and you may have heard them before. However, as the world becomes increasingly more digital, the probability of being hacked also increases. So, it's always good to have a refresher. We have found it best to talk regularly and non-threateningly to family members and office colleagues about the topics above, as this helps to build safer practices and appropriate usage patterns. When your children are young and just beginning to access the internet, be open with them about the repercussions that can arise from what they do and say electronically. Teach them to be thoughtful in their use of social media and how they appear and continue those family discussions right into adulthood.

If you have a small business or sole proprietorship, or if you have a multigenerational and dispersed family, it might make sense to hire a qualified IT firm to set up your email, your home network, and your general IT security systems including backups. An additional benefit from hiring an outside firm is that you'll have someone you can call for help if you are hacked, hit with ransomware or lose any files.

Stefan is the Director of Technology and a Principal in the New York office. He is responsible for the ongoing development, release management, and supervision of the firm's technology platform.

Pierre is a Partner in the New York office and has more than twenty-five years of experience founding, investing in and providing strategic growth advice to early-stage and middle-market companies. In addition to mentoring executives, Pierre has advised business-owning individuals and families on the personal/ownership side, as he has experienced many inheritances and business-ownership situations in his own family.