Your Online Security

You think it will never happen to you, but our office experienced an attempted security breach on a client's account first-hand. A while back we received an email from a client requesting a full withdrawal of all their funds. Common sense and our policies state all requests like these can only be authorized verbally. A short while later, we received a call from an individual, claiming to be the client, requesting the same: a full withdrawal from the stated account. When we tried to verify their identity, the caller was unable to give the correct information. It was clear from the beginning that this request was not made by the client and we did not comply. We confirmed the security breach with the real client, which stemmed from a hack of their free email account.

Although many of the steps we take may seem unnecessary or over-the-top, we take them because your security is extremely important to us. According to the Federal Trade Commission, identity theft has impacted millions of Americans and continues to be the fastest growing crime in the US. While browsing the internet, shopping online, or checking your accounts, your personal information is vulnerable to hackers, spammers and scammers. There are simple steps to take to protect your data. It all comes down to managing to whom you give information and how it is delivered.

7 SIMPLE STEPS FOR ONLINE SECURITY

1) Verify Sources

Be aware of to whom you give personal information and how your information will be delivered. Typically, legitimate businesses will never reveal or request sensitive personal information over unsecured connections. They will use encrypted emails and secure websites to send or receive sensitive information. If the company you're doing business with does not have a secure method of sending and receiving information, request the information to be delivery in a hard copy method. While e-mail technology is convenient, it is not always the safest way to conduct business.

2) Use Bookmarks

Did you know that websites or hyperlinks can also be impersonated or hacked? Hackers can create legitimate looking websites for companies you regularly do business with and use these sites to gather sensitive data from you. For example, you may receive an e-mail from the major bank you do business with asking you to click the link and log in to view important information. If you click on the false link and attempt to log in by submitting login or personal information you have potentially given your information to scammers. While links are helpful tools, bookmarking commonly used webpages and using those bookmarks to access them helps protect you from false links.

3) Use Strong Passwords

One of the best ways to protect your data is by using strong passwords. A strong password should start from the moment your computer turns on, by ensuring you have your computer or device password protected. The Federal Trade Commission (FTC) recommends setting passwords at least 10 characters long, including letters, numbers and special characters, (#$*&^). The longer the password, the tougher it is to crack. With that said, a password is only secure as long as it is a secret. Never keep passwords written down near your work station or within your email system. Utilizing a password keeping program is a good option to manage numerous login credentials. Some password keeping programs also help create strong 10 character or longer passwords for extra security.

4) Auto Update

The bad guys constantly develop new ways to attack your computer, so your security software must be up-to-date to protect against the latest threats. Most security software can update automatically; set yours to do so. You can find free security software from well-known companies. Also, set your operating system and web browser to update automatically. It's important to run regular antivirus scans as well. If your computer does not stay on overnight, you should set a reminder for yourself to run a scan on a regular basis.

5) Back Up Your Files

Backing-up your computer files regularly is a great way to protect your information from a hard drive failure or theft of your computer or device. Using a reputable off-site backup provider is typically the easiest way to regularly back-up important files without a great deal of effort on your part. It's also typically easy to recover your data after a loss. If your computer is compromised, you'll still have access to your files and be able to return to normal activities quickly with less stress.

6) Beware of Hot Spots and Wireless Access

We live in a society where responding to e-mail or shopping on the web is as close as your smart phone or tablet. Whether you're meeting a friend for coffee, staying in a hotel, or waiting for an airplane, we like to stay connected. Often many of us turn to wireless hot spots to increase speed or to just save on our data usage, but sometimes, without you knowing, hot spots are being monitored by hackers looking to access your personal files, credit card information and more. Being aware of where and how you access the internet is critical in protecting your safety. When in doubt, experts recommend to use your 3G or 4G data for the most secure internet connection while away from home or the office.

7) Monitor your Social Media and E-mail Settings

Hackers are constantly changing the scams the use. Service providers do their best to keep our information safe: they require strong passwords, they ask security questions and lately they're asking for our phone numbers so they can verify our information via a text or phone call code. Now hackers are now getting into our social media and e-mail accounts, changing our security settings and manipulating our accounts just enough to be a benefit to them, but not enough for the unsuspecting user to notice. One of the first things they do is change the security words or phone number linked to the account to ensure they have access over you. To protect yourself from this latest concern, be aware of your security settings and check them often.

For those of us who are not as computer savvy as our children or grandchildren, the most important thing to remember about internet safety is, when in doubt, take extra measures. Verify links via your bookmarks, call and talk to a legitimate customer service representative instead of responding to an e-mail and be smart about your conduct online. Sitting alone in front of a computer can give you a false sense of privacy, but remember, you're sharing the internet with millions of others. You would never drape a sign with your credit card information around your neck while walking the mall, so think of the internet as a great big shopping mall, where everyone can see you, and protect yourself appropriately.

This article written by Sandra J. Wagner, CFP®. Sandra has been helping people with their finances since 2001. She is a CERTIFIED FINANCIAL PLANNER™ professional and CEO of Wagner Planning.

Back to Top More Articles