5 Steps for Protecting Your Personal Information

It seems every few months a new report surfaces of confidential information being hacked. We must take steps to protect our personal information ourselves, but knowing what to do and where to turn can be challenging. The following are some practical steps you can take to keep your important personal information secure.

1) Share Carefully

Scammers will say anything to cheat people and telemarketing scams are quite common. One specific scam is a caller claiming to be the IRS and telling you that you owe taxes. The caller threatens that if you do not provide credit card information for payment immediately, you will be arrested. Please know, the IRS will always mail you first and will not request a credit card payment over the phone or threaten arrest. Another type of phone scammer is much nicer using phrases like "you've been selected" or "you've won." Threatening or kind, callers trying to get you to provide money or information are scams. The best thing to do with these calls is to simply hang up. If you are unsure if the call is legitimate, ask for a case number and call the company back from a verifiable phone number.

Being cautious on the phone is just one way to keep your information safe, but you also must be aware of how your information is transmitted over email and the internet. Legitimate businesses should never reveal or request sensitive personal information over unsecured connections. They should use encrypted emails and secure websites to send or receive that type of information. If the company you're doing business with does not have a secure method of sending and receiving personal information, request the information to be delivered in a hard copy. While e-mail technology is convenient, it is not always the safest way to conduct business. Bottom line is you should never give out personal information unless you initiate the contact or verify the source and do it securely.

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 a major bank where you have an account asking you to click on a link and log in to view important information. If you click on the false link and attempt to log-in by submitting your 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 those websites helps protect you from false links.

3) Use Strong Passwords

One of the best ways to protect your information is by using strong and unique passwords for every website you visit. When hackers steal login information from a company, they often use those credentials to try to access other sites. Having a strong and unique password for every website lessens the chances your account will be accessed. The Federal Trade Commission (FTC) recommends setting passwords at least 10 characters long, including letters, numbers and special characters, (#$*&^). Consider using a phrase or substitute numbers for some words or letters. 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) Don't Overshare Online

Hackers are constantly changing the scams the use. Service providers try to keep our information safe by requiring strong passwords, asking security questions and lately asking for our phone number to verify our information via a text or phone call code. To ensure these extra measures successfully protect your data, be aware of what you post on social media. The more you share publicly, the easier it is for hackers to potentially access your data. For example, if you post where you went to high school, and a security question is your school's mascot, it is rather easy for a hacker to figure that out.

5) Watch Your Credit

Recently, many have had their financial information compromised due to various data breaches. One way to reduce the risk of identity theft is to freeze your credit, (also known as securing your credit). For a nominal fee, you can file a request to each credit agency, (Equifax, Experian and Transunion) and if someone tries to take credit out in your name, they will be denied. Should you need to open a credit account, you can request the freeze to be lifted by contacting the credit agencies.

Whether you freeze your credit or not, it is important to regularly monitor your credit report for accuracy. You are entitled to a free credit report from each major credit agency every 12 months and can request it by going to annualcreditreport.com. While it may seem like a hassle to request reports from all 3 agencies, there may be different or erroneous information at one agency and not another. If you find any incorrect information, it is imperative you report the issue and take necessary action immediately.

While there is no way to be completely protected from identity theft, following the above guidelines will help you do your part to keep your sensitive information safe.

Rebecca Magby is the Operations Manager for Wagner Planning and been working for Sandra J. Wagner, CFP® and Wagner Planning since 2009.

Back to Top More Articles