CREATIVE PLANNING

February 6, 2019

10 Ways to Protect Yourself from Digital Threats

Peter Mallouk
JD, MBA, CFP®
President

The multitude of connected devices, social media sites and online shopping sites have fundamentally changed the way we interact with the world around us.[1] Each passing year brings new ways to connect to friends, businesses, and others in ways we never previously imagined. But with each new connection, we increase the risk that our private personal information will fall into the wrong hands. With news of data breaches and hacking victims making the rounds more and more frequently, it can feel like the only way to stay safe is to completely unplug.[2]

The good news is that there are still many ways to protect yourself that don't involve living in a bunker with a flip phone. Below are some tips from cybersecurity experts to help keep you and your family safe in the digital world.

1. Use a passcode on your phone.

When you stop and think about it, your smartphone is the holy grail of personal information for a hacker. Going to be out of town? It's on your calendar. Need bank account numbers? They're in your banking app. Want to reset account passwords? It can be done via email. The list goes on and on.[3] This alone should get you to password protect your phone, one of the easiest ways to protect yourself. You can also set up the ability to remotely delete the data off your phone. If it is lost or stolen, you can then take steps to keep your information away from hackers, even if they are able to break your passcode. Establishing a phone passcode is a no brainer, and if you aren't doing this, God be with you.

Call us:
866.909.5148

Email us:
cpi@creativeplanning.com

Visit us online:
www.creativeplanning.com

2. Be careful with email links.

One of the most nefarious scams going is the 'phishing' scam. You receive an email that looks like it came from your bank, credit card company, or a major company you likely do business with online, like Apple, Amazon or Netflix. The email says that you need to update your

[1] And have certainly changed the way my teenagers interact with me!

[2] And move deep into the forest with nothing but a tent, basic cooking supplies and a self-generating power source.

[3] And a good portion of phone users have, shall we say, at least one very personal photo on their phone.

payment information in your account, and it provides you with a handy link to do so. You click on the link, go to the site, and provide your credit card information or social security number. The problem is, that wasn't the real site. It was a fake site set up by hackers that looks real enough to convince you to hand over the goods. Nothing is more depressing than finding out you proactively handed over your personal information directly to a thief. The best defense? Don't click on links in an email message; instead, go to the company's web page directly, and follow the proper steps from there.

3. Use strong passwords.

When hackers want to try to find your password to a website or computer, they don't try whatever password combinations they can think of for hours on end. Instead, they rely on powerful computer programs to generate hundreds of thousands or even millions of words plus other combinations of letters and numbers. No matter how clever you think it is to use "1234" as your password,[4] you won't outsmart the machines. Instead, use passwords that are made up of upper-and lowercase letters, symbols, and numbers. Longer passwords are more secure, and the best ones are a random string of characters. There are online password generators you can use for ideas, and many even provide a handy mnemonic device to help you remember it. If you are looking for something hard to discover but easy to remember, make your password a phrase or song you like, replacing some letters with symbols.

4. Don't use the same password for every account.

Let's face it: passwords are a nuisance, and it seems like everywhere you go online, you are being asked to create one. The easiest solution would be to use the same password everywhere for convenience, but the trade-off is reduced security. If one site gets broken into, the hacker now has the password that gives them access to your entire digital life. When the hackers successfully determine one of your passwords, they will then take that password and attempt to access more critical sites, such as your bank account, investment account, etc.[5] Always use unique passwords for important sites, such as banking sites, email, etc., and change them every six months. If you have a lot of passwords to keep track of, consider using a password manager in your web browser. This way, you only have to remember one master password, while keeping all of your unique passwords securely at your fingertips.

5. Be wary of public networks.

Open Wi-Fi hotspots are springing up in more and more places, from your doctor's office to your favorite restaurant. While the appeal of free, fast internet is undeniable, these networks

Call us:
866.909.5148

Email us:
cpi@creativeplanning.com

Visit us online:
www.creativeplanning.com

[4] Or its close cousin 'password 1234'.

[5] So while you may shrug when you hear that one website you visit like 'adorablecatvideos.com' gets hacked, just know the hackers will likely take the info they uncover about you and try to get into your bank accounts.

have a major flaw: they are not secure. It's very easy for a sophisticated hacker using the network to trick your phone or computer into sharing everything you do online, including passwords, credit card numbers, and more. Avoid shopping online or accessing password protected sites, such as your bank accounts or email, when you are on a public network. If you need to access a protected site, use your cell phone network rather than the Wi-Fi network. If you are working away from the office, see if your company offers a virtual private network (VPN), which secures your data while you are online.

6. Stay up-to-date.

Online security is like a game of chess: the bad guys find a way to get people's data, then the technology companies come up with a fix. The bad guys find another way in, which leads to another fix, and on and on basically forever. One of the ways the technology companies fix these breaches is updating operating systems, apps, web browsers, etc. You are only protected if you install the updates[6]. Using outdated software is the equivalent of leaving your back door wide open for criminals to walk in and take whatever they want. You can set your phone or computer to automatically install updates when they are available[7] so you know you are always using the latest version.

7. Practice good offline security habits.

The strongest password in the world is useless if it's written on a note you've stuck to your monitor (and no, inside your desk drawer is not a better option). Keep any sensitive information, account numbers, social security numbers, etc., that could be used to gain access to your online accounts locked away from prying eyes. Also, be aware of your surroundings if you are entering a password or credit card information on your phone in public. Someone standing over your shoulder on the subway or sitting next to you on a plane could have a perfect vantage point to see what you are typing into your device.[8] Keep portable devices, like laptops and phones, locked with a password when not in use, and never leave your electronic devices unattended in a public place.

8. Stay private on social media.

Sometimes hackers don't have to go too far to find the information they need to take advantage of you. Many people conveniently post about it online through social media sites.[9] Don't make your private information public. Take advantage of the social media site's security settings to restrict who has access to your information. While you're at it, avoid

Call us:
866.909.5148

Email us:
cpi@creativeplanning.com

Visit us online:
www.creativeplanning.com

[6] Much like the dumbbells my kids bought me for Christmas only work if I use them.

[7] I wish there was something that would automatically work out for me too.

[8] Yes some crooks are still kicking it old school, using less sophisticated, but just as effective, ways of stealing from you.

[9] Don't post things like 'we are having so much fun in Cabo! Only 4 days left to enjoy the sun! If you are a criminal, just know I will be back then, so steal all my stuff as soon as possible!'

the survey apps you see those sites, as most are designed to entice you to share your profile information with someone who will promptly sell it.

9. Don't allow your personal information to be used against you.

Many times, hackers don't have to use sophisticated tools to get into your accounts. If a site offers password recovery questions to grant access, the hacker may be able to find the correct answers to those questions online. Common password recovery questions include your high school mascot, the make and model of your first car, your mother's maiden name, etc. Some or all of these answers may be easily found on social media profiles or through a quick Google search. The simplest solution is to set up your account with made up answers. If you say that your mother's maiden name was 'Catwoman' or your high school mascot was a Ford Pinto, there's no way for the bad guys to use the truth against you.[10]

10. Take advantage of enhanced login security tools.

An increasing number of sites are starting to offer enhanced login security tools, like two-factor authentication, to help protect their users. Texting or emailing a code to your cell phone or email to complete the login process provides an additional layer of protection. This gives you two advantages: one is that even if someone obtains the password to the site, they won't have any way to get the code they need to complete the login. The second is that you will be notified via text or email anytime someone tries to log into the site. This gives you the opportunity to change your password and notify the site of the attempted attack. You should absolutely use two-factor authentication every time it is offered to you.

There is no single foolproof method to prevent all online attacks. But hackers are like any other predators: they seek out the easiest and most vulnerable targets to attack. By taking these simple steps, you become a much less appealing target, making it more likely that the bad guys will look for an easier, less informed target.

Call us:
866.909.5148

Email us:
cpi@creativeplanning.com

Visit us online:
www.creativeplanning.com

We appreciate your confidence in us and welcome introductions to friends, family, and colleagues.

[10] If your mother's maiden name is in fact Catwoman, you have bigger problems than the ones we are covering here.