NOYES CAPITAL MANAGEMENT® LLC
Personal Financial Planning & Prudent Investment Management
17 Village Road, New Vernon, NJ 07976-0271 + 973-267-8120

Internet Security – It's Everyone's Problem

By Cynthia Aiken, CFP® and Rachael Williams

You are a candidate to be hacked. If it hasn't happened yet, then it probably will. 73% of all Americans have fallen victim to some type of cybercrime. Over 27 million Americans have been victims of identity theft over the past five years and nine million of them had their identities stolen in the last year. Here are several different ways that criminals can get your personal info and what you can do to prevent theft or repair your security.

Hackers frequently use email to get their victim's data. In our office, a client's email was hacked and the hacker sent an email to our office requesting account balance information and transfer of funds to a foreign account. The client was unaware of the emails to us and the request for transfer. Fortunately, we suspected that it was a bogus request and contacted the client.

Cyber criminals are increasingly using websites to distribute their nasty code. On average 30,000 new websites are identified every day distributing malicious code to any users. Many sites are legitimate businesses that unwittingly distribute malicious code. Last week we found a fake Adobe site in a Google search result. Just by visiting a website, your devices can be compromised.

Heartbleed, a recently uncovered hack, impacted hundreds of popular websites and services and could have quietly exposed your personal account information. Heartbleed is a software bug that is used to steal encryption keys in software that powers many of the services we use daily. Gmail, Yahoo email, Facebook, Instagram Pinterest, Tumblr, Google, Yahoo, Etsy, GoDaddy, Flickr, Netflix and YouTube were all compromised. Changing your passwords on these services will protect your data going forward.

Mobile devices are vulnerable to social media scams and malware. Mobile malware increased 33% from 2012 to 2013. Mobile users are highly susceptible to hacks via mobile apps on both Apple and Google's platforms. The most concerning hacks are those targeting financial and shopping apps because users entrust them with essential account numbers and passwords. Many apps are not secure and may leak device ID, location, photos and browsing history. Furthermore, mobile devices often do not have security software, so they lack protection against these attacks.

Don't lose control of your mobile phone. Mobile phones are mobile, so they can easily be misplaced, lost or stolen. Your cell phone serves as an access point to your online identity and can be compromised allowing a hacker to use your cell phone as a cheat sheet for all your online accounts. If a hacker learns your Apple ID and password, they can remotely control your phone and lock you out. Recently, hackers remotely locked iPhones and iPads in Australia, through compromised iCloud accounts and then demanded ransom payments to unlock them.

Protect yourself. What can you do to avoid or reduce the probability of attacks?

1. Change your passwords and make them long. It takes only 10 minutes to crack a lowercase password that is six characters long. Add two extra letters and a few uppercase letters and that number jumps to three years. Add just one more character and some numbers and symbols and it will take 44,530 years to crack your password.

Don't use the same password for more than one purpose. Change passwords quarterly.

2. Keep your operating systems updated on all your devices. Uninstall software and apps that you no longer use.
3. Get protected and stay protected. Use protection from spyware, malware and viruses. Purchase and use a brand name product. If your computer or other devices have a firewall, then keep it updated.
4. Only visit secured sites. Websites starting with https – s is for secure. Download and install this fee safeguard at https://www.eff.org/https-everywhere.
5. Never open an email – especially an attachment – from an unknown source. Be careful if email from a friend looks suspect.
6. Take caution when clicking links and downloading software. Free or discounted software may have been tampered with, so remember that you may get what you pay for.
7. Be careful what you put on your phone. Always use reputable apps from official platforms and app stores. We recommend software security systems for apps which guard against malware or viruses, such as Arxan, which detects attempts to tamper and prevents execution if found.
8. To protect your Apple ID, iPhone, iPad and iCloud accounts, use unique, long passwords and update security and operating systems for each device/account. Download the "Find My iPhone" app so that you can locate and lock your phone or tablet remotely if it is lost or stolen.
9. If buying a new phone, computer or tablet, eliminate your personal data before you recycle, trade in, sell or donate your aging device. Start by backing up any files you want to keep then do a factory reset on your phone or tablet and delete data and reformat your computer hard drive. Erasing isn't really enough on your computer, so remove storage and do a secure wipe.

Too late! You've been hacked – now what? If your email has been hacked, there are several steps you need to take now.

1. Reset your passwords immediately – do not reuse passwords. Create different passwords for each account and write them down or save them in a password app for safe keeping.
2. Run the most recent version of your operating system, anti-virus and antimalware programs to scan for malware and viruses. In our office, Malwarebytes.com has saved the day several times by getting rid of imbedded marketing software and pop-ups.
3. Report the incident to your email server. Email providers hear reports of hackings daily and may be able to provide details of the attack and make suggestions for repair and future protection.
4. Check your linked accounts. Typically, email ID and passwords are used for multiple online accounts including social media, banking or shopping. Check your email Inbox, Sent and Trash folders for emails indicating password resets from any online services. Hackers frequently reset user names and passwords to access your information without your knowledge.
5. Check email rules and filters to be sure that nothing is being forwarded to another account. Review your Spam and Sent folders for any uncharacteristic messages.
6. Follow the money – check that no new shipping addresses have been set up on your accounts, no new payment methods have been added or new accounts linked.
7. Lock down your credit – contact the three major credit reporting agencies, put them on alert and have them freeze your credit.
8. Subscribe to a credit monitoring service such as IdentityGuard, CreditReport123 or PrivacyGuard which alert you if there are any major changes or discrepancies on your credit report, so you can alert authorities.
9. If you still cannot eliminate the hackers, the only solution is to reformat your hard drive and reinstall your software.

No, your online identity won't ever be bulletproof, but it is imperative that you are aware of security threats to your online identity and take steps to prevent your info from being hacked. If you are attacked, immediately repair the damage and implement safeguards to prevent further attacks. By protecting your online identity and passwords, you increase the security of your online life, decrease digital anxiety and avoid becoming a victim of cybercrime. Stay safe!