Private Person

In this article we will talk about internet security as a private person. We are going to tell you why you are not safe while being online. We will also tell you what you can do to prevent hackers from getting an easy hold of your information. Now we will analyze some schemes that have to do with identity theft and later on we will give you some advice on how you can prevent yourself from having your identity stolen. Your identity cannot only be stolen by hackers but it can also be stolen when someone fooled you to give him private information that concern your credit card number, Social security number etc.

Socialmedia danger

Because people often post detailed and specific information on Facebook (including phone numbers, addresses, class schedules, social plans, etc.) you can be more easily stalked by strangers (or even acquaintances).
Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements and via third-party apps. On Twitter, shortened URLs (popular due to the 140-character tweet limit) can be used to trick users into visiting malicious sites that can extract personal (and corporate) information if accessed through a work computer. Twitter is especially vulnerable to this method because it's easy to retweet a post so that it eventually could be seen by hundreds of thousands of people.
Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information.
Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites.

E-mail theft

Phishing is a scam where Internet fraudster send e-mail messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victims' identity. Current scams include phony e-mails which lure the victims into the scam by telling them that there is anything not ok with their accounts (Bank, Facebook,..).

Clone phishing is a type of phishing attack that when an email is being sent, it contains an attachment or link that has its content and recipient address taken and used to create an identical email. The attachment or link within the e-mail is replaced with a malicious version and then sent from an email address to appear to come from the original sender.

Mail theft is when someone targets your mailbox and removes mail that has sensitive and private information on it. In that way the thief can take your credit card bills, bank statements and pretty much anything that can be used to steal your identity. At times, identity theft criminals have been known to re-route your mail without your knowledge or permission by submitting a change of address to the post office.

Social Engineering

Social engineering is when someone who is either in person or over the telephone, or computer who tries deceive someone else into exposing sensitive information. Usually, social engineers know some information that lead the victim to believe that they are legitimate and give the information asked.

Shoulder Surfing

This attack may occur anytime you use a password or a device that stores PIN numbers, such as at an ATM. The identity thief attempts to get close enough to you in order to record your password information when you enter it, such as a PIN number. Although this can usually occur in a public setting, where the victim is and their credentials are in plain sight, it may also occur through a video camera that has been setup by the criminal.

Skimming

This can happen anytime you use your credit or debit card. The theft takes place when the device which reads your credit card information from the magnetic strip or from the chip on the front of the card. This allows the criminal to make a copy of your card to make unapproved purchases. Skimming can occur through many different ways, whether it is a recording device set up on an ATM machine or a salesman who secretly swipes your card onto his personal digital card reader.

Pretexting

Pretexting is when the thief has done prior research on your personal information, and uses this information to lure you to give him more sensitive information, such as a credit card number or Social Security Number. The intriguer will call you on the telephone, and lead you to believe they are a business that requires this information. Most people tend to believe them, since they have their name, address, and telephone number.

Real Case

One good advise to keep your life private from hackers is, don´t link accounts. When Mat Honan suffered a hack of his entire digital life in 2012, his Google account was taken over and deleted. At the same time Honan´s Twitter account was compromised by hackers, and used as a platform for racist messages. In a interview he sad it was in many ways his own fault, because all of his accounts were daisy-chained together. When the hackers get into Honan´s Amazon it did it possible for them to get into his Apple ID and which helped them get into his Gmail. Honan also sad that if he had used two-factor authentication for my Google account, it is possible that none of this would happened, because the hackers goal was to take over his Twitter account.

How to protect yourself against hackers

Have individual passwords on all your password protected pages.

- Have random passwords, with capital letters, regular letters and numbers. It should also be at least twenty digits long.
- Make fake answers to the security questions. Eks. What is your favorit food? And your answer can be something like hippo-campi meat.
- Whenever possible, use your fingerprint as an extra ID.
- Hide your password whenever you have to type it in public, preventing people to se it over your shoulder. You should also be aware of cameras in the ATMs, and hide your password from those to, it may be set up by someone dishonest.
- Never have the bank or other public instances who have sensitive information to you send it in the Mail, always go and collect it in person, this way it will not be lost of misused on the way.
- If the bank or other public instances calls you to get information, never giv it over the phone, it may not be the bank, or it may be people listening in on your phone calls. Always go to the bank or other public instans to gave the information i person. Than you will also know if it really was the bank, or someone trying to Get your information.
- Never public embarrassing photos of your self or others in social media. The internet never forgets, an some one might try to use it against you.
- Never reveal to much personal information about your self, people can use it to gagn access to your accounts. Even smal bits of information that you think is unimportant can be used to gain access, like your mothers maiden name.
- Never upload sensitive photos, videos or information to a dropbox, have those on a separate devise that is not connected to the internet.
- USB drives are not always safe. Never upload sensitive information on to one, unless you are certain that it is safe. And for the love of God, NEVER lose one if you have something on it!
- Always update your devises, their might be security updates.
- By an kinda expensive antivirus program, those are better Than the free ones. never ignore Ann request to update it.
- Change your passwords regularly.
- Report suspicious emails and internet sites/links.
- Never send personal/sensitive information on email.
- Monitor your mailbox, Get your Mail every day, and put padlock on your mailbox.
- Periodically check your credit card and debit card reports. At least ones a month.
- Secure your wi-fi. Use the security key, those are random.

Made by

Andreas
Anthony
Adrian
Lovisa
Malene Kristin