identityfinder

Identity Finder Student Initiative *Security Tips*

In the spirit of the upcoming holiday season we are also providing you with a few tips to stay safe while shopping online and to protect your computer. We hope this "Top Twelve" list keeps you secure and one step ahead of the criminals!

- Avoid Phishing Attacks: Before typing your username and password to enter a site, make sure the website address is correct. Do not click on links from e-mails you receive. Microsoft acknowledged in October that over 10,000 Live Hotmail accounts were compromised by a phishing scam.
- Don't trust "scareware": Do not click on advertisements claiming you might be infected with a virus. Rogue ads recently started popping up on sites like The New York Times that purport you have a virus only to trick you into downloading malware. Rely on your system anti-virus for this – free from Apple or Microsoft or available from other vendors.
- Beware Who You Friend: Fake profiles have become very popular on social networking sites like Facebook. Holiday time is an excuse for people to purport they want to get back in touch. Protect the privacy of your profile by rejecting anyone you do not know. Do not post your full birth date including the year.
- Don't Shop in Public (online!): If buying something online, use your own computer. Don't use public computers while on vacation at hotels or airports. Public computers can have keyloggers that record your information as you type it.
- Create Complex Passwords: When creating passwords at stores, use upper and lower case with numbers. Use at least seven characters and don't choose a word from a dictionary. Passwords can be guessed very quickly by hacker programs. If you need help remembering all your different passwords, use a Password Vault or Manager to secure them all.
- Always Update Definitions: Anti-malware programs such as anti-virus or anti-spyware can only detect malware for which they have definitions. Download the latest definitions whenever they are available to prevent brand new attacks.
- Use SSL (aka the padlock!): A term you might not have heard of, but you probably have seen that little padlock in your web browser near the address bar or in the bottom right corner. Make sure it's there when entering personal information as it indicates your information is protected. Do not press submit if there is no padlock at a store.
- Install Latest Software Upgrades: Upgrade your operating system, web browsers, and media applications with the latest versions. Hackers are always looking for ways to create new holes in existing software so they can steal your data. Software vendors patch these holes with upgrades. A recent banking Trojan stole money after infecting web browsers.
- Don't Give Personal Information Over Live Chat: When shopping online you might see a Live Chat window appear letting you ask questions to a customer representative. Never give them your credit card number or other personal details.
- Check Your Credit: Visit annualcreditreport.com (and not other knock off websites with similar names) before and after the holidays so you can verify no unauthorized credit cards are opened under your name and no large purchases were made without you knowing. Your credit report shows all your accounts and overdue balances.
- Use Onetime Credit Cards: If you aren't familiar with a store, use a virtual credit card that expires after one use. Some websites masquerade as shops but really just steal your credit card numbers.
- Protect Your Identity: Do not keep unprotected copies of your identity on your computer. Most people have typed their Social Security Number into an application or Credit Card number into an e-mail but forgot it was saved in their computer. Use Identity Finder Free or manually search your computer to find and protect anything that could be used to commit identity fraud if seen by a hacker.

Copyright © 2010 Identity Finder, LLC. All Rights Reserved. Identity Finder and the Identity Finder logo are trademarks of Identity Finder, LLC.