The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Overview
- Why You Are Targeted
- Protecting Yourself

Yes, You Actually Are A Target

Overview

A common misconception many people have is that they are not a target for cyber crime: that they or their computers do not have any value. Nothing could be further from the truth. If you have a computer, mobile device, an online account, email address, credit card, or engage in other type of online activity, you are worth money to cyber criminals. In this newsletter we explain why you are a target, how you are being attacked, and what you can do to protect yourself.

Guest Editor

Eric Conrad is President and CTO of Backshore Communications and is lead author of the books the CISSP Study Guide, Second Edition and the Eleventh Hour CISSP, Second Edition. He is also the coauthor of the six-day Continuous Monitoring and Security Operations (SEC511) course at SANS.

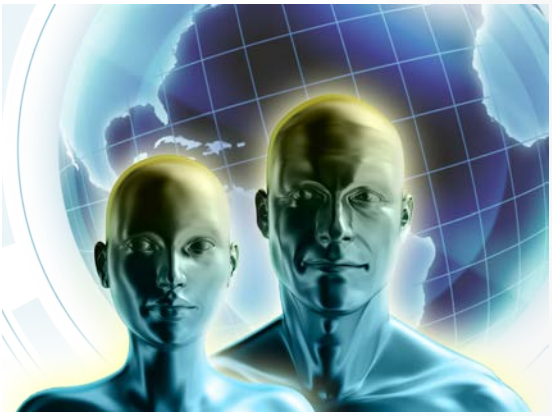
Why You Are Targeted

Crimes such as fraud, identity theft or extortion have existed for as long as there have been civilizations, they are a part of our daily lives. A criminal's goal has always been the same: to make as much money as possible, as easily as possible, and with as little risk as possible. Traditionally, this was difficult because criminals were often limited by their location and had to physically interact with their intended victims. This not only limited whom criminals could target, but also exposed criminals to a great deal of risk. However, crime has radically changed with the advent of the Internet and online technology. Now cyber criminals can easily target almost everyone in the world, with little or no cost, and at very little risk. Additionally, cyber criminals have become highly organized and efficient, enabling them to be more effective than ever.

Ultimately, cyber criminals know that the more credit cards they steal, the more bank accounts they hack, or the more passwords they compromise, the more money they can make. They will literally attempt to hack anyone connected to the Internet, including you. Hacking millions of people around the world may sound like a lot of work, but it is surprisingly easy as they use automated tools to do all the work for them. For example, they may build a database of millions of email addresses and use an automated tool to send a phishing message to every one of those addresses. Sending the emails costs the criminals almost nothing: they simply use other hacked computers, perhaps even yours, to do their dirty work. This is also another example of why your devices

Yes, You Actually Are A Target

have value, if nothing else they can be used to hack or harm others. Ultimately, these criminals do not know who will fall victim to their email attacks, but they do know the more emails they send out the more people will eventually fall victim. Or perhaps the criminals will literally scan every computer on the Internet (once again using hacked computers to do the scanning), looking for any computers or devices they can hack into. Remember, you are not being singled out because you are special. Rather, these criminals are targeting everyone they can, which happens to include you.



You may not realize it, but your devices and your information have tremendous value to cyber criminals around the world.

Protecting Yourself

When cyber criminals attempt to hack people around the world, they are typically using relatively simple methods. Fortunately, by following some equally simple steps you can go a long way towards protecting yourself. Some steps we recommend include the following:

- Yourself: Ultimately, you are the first line of defense against any cyber attackers. Many attacks begin with a cyber criminal trying to trick or fool you, such as tricking you into opening an infected email attachment or fooling you into giving up your password over the phone. Common sense is your best defense: if something seems odd, suspicious or too good to be true, it is most likely an attack.

- Updating: Make sure that any computer or mobile device you use is fully updated and has all the latest patches. This is not only important for your operating system, but for any applications or plugins you are using. By always keeping your systems and applications updated you help protect yourself against the most common attacks.

- Passwords: Use a strong, unique password for each of your accounts. That way when a website you use gets hacked and all the site's passwords are compromised (including yours) your other accounts are safe. Also ensure that all your different devices are protected by a strong, unique password, PIN or some other type of locking mechanism. To securely keep track of all your different passwords we recommend you use a Password Manager.

Yes, You Actually Are A Target

- Credit Cards: Check your financial statements often, we recommend at least weekly (monthly is not enough). As soon as you see any unauthorized transactions on your credit card, report it immediately to your card issuer. If your bank allows you to set email or text message alerts for unusually large or odd transactions, use them for even faster notification of suspicious activity.

- Your Network: Secure your home network Wi-Fi access point with a strong administrator password and ensure your Wi-Fi network requires a password for anyone to join it. Also ensure that that you know what devices you have connected to your home network and all those devices are updated.

- Social Media: The more Information you post online the more likely you may put yourself at risk. Not only can any information you post make it easier for cyber criminals to target and fool or trick you, but any information you post may actually identify you as a more valuable target.

Become a Security Professional - SANSFIRE 2014

SANSFIRE 2014 will be held in Baltimore, MD on June 21st - 30th, with over 40 of SANS's top security courses taught by top-rated instructors. In addition, this is our annual "Internet Storm Center Powered" event. Each evening, the ISC handlers will share riveting talks on their most interesting experiences and the latest cyber threats. For more information, please visit http://www.sans.org/event/sansfire-2014/welcome/.

Resources

OUCH! Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Securing Your Home Network:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Poster: You Are A Target:	http://www.securingthehuman.org/resources/posters

License

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus