SANS SECURITY

The Monthly Security Awareness Newsletter for Computer Users

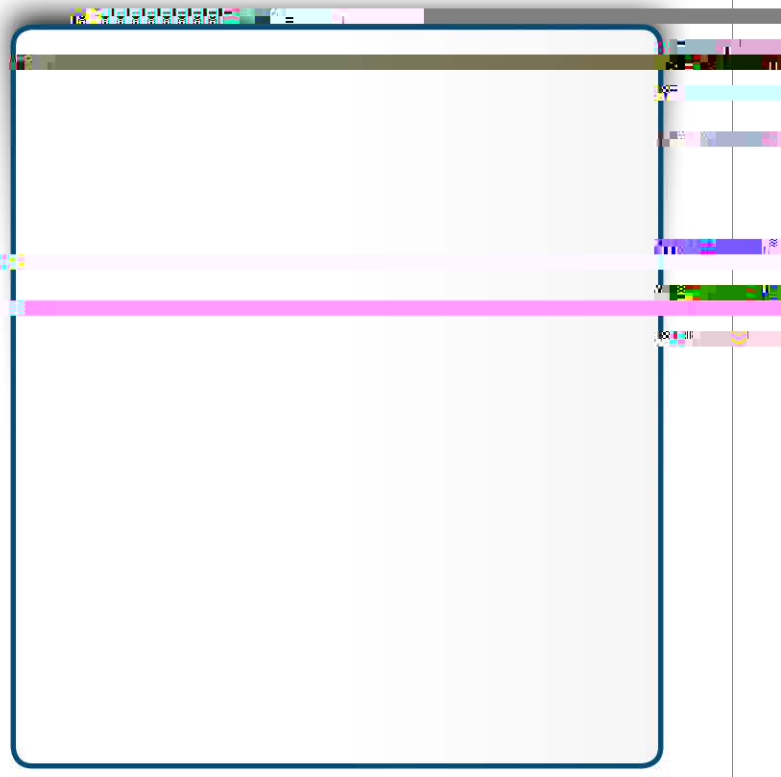
OUCH!

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.

© The SANS Institute 20

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.



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

- 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

© The SANS Institute 2004