Finance New Mexico

Article 236 April 9, 2012

How Businesses Can Protect Themselves From Hackers

By Caroline Dennis, President, Wired Nation

Given the numerous products and promises of the information technology (IT) security industry and the frequent news stories about data breaches, it's not surprising that business owners don't know where to start when it comes to protecting themselves from information-highway robbers. Some wonder why they should spend money on sophisticated security systems when hackers can get around them.

Even if a business doesn't hire someone to watch over its systems, it can implement some basic IT security measures to significantly reduce its vulnerability.

Know the Enemy

Small businesses often deceive themselves into thinking hackers won't hurt them because hackers are after big money from big businesses. But small organizations are perfect targets because hackers know that small businesses typically have minimal security. Hackers likewise prey on business travelers — especially executives — who use unprotected mobile phones, Blackberrys, iPads and Kindles to conduct business.

Hackers get into computer systems in several common ways. They can extract information about a business by gaining the confidence of an unsuspecting employee, which is why staff members need regular training about basic IT security practices. Hackers know that companies have lots of software running on their computers, and most of these computers are not patched and updated regularly, making them vulnerable to the malware or keystroke logging programs hackers use to steal account information. And weak passwords are easy for cyberthieves to crack.

How to be More Secure

A business owner should first identify what data or intellectual property is most important to protect based on the potential impact of its loss or corruption. To begin protecting it, he should:

Strengthen passwords: People often use the same simple password on multiple sites because it's hard to keep track of dozens of them. The free program Password Safe (http://passwordsafe.sourceforge.net/) offers a way to store, generate and manage passwords. (A password can still be stolen by keystroke logging malware, but this is a risk for any password-protected asset.)

Use encryption programs: Businesses that use services like Dropbox or search engines like Google should know that any information launched into cyberspace is out there for public consumption. SpiderOak (https://spideroak.com/) is a free online backup, synch and sharing program that encrypts, or scrambles, the data on a computer before it's uploaded to the Internet. It works with Windows, Mac and Linux operating systems.

Monitor computer logs: A company's firewall, server or router generates logs that require regular monitoring, as they usually give the first warning of intrusions or suspicious activity. If the business doesn't have time to monitor these systems, it can hire a managed service provider to keep watch and perform regular patching. Log management software packages are another way to catch a problem before it becomes severe and costly.

Encrypt files sent by email: Sensitive documents sent via email can expose a business to hacking. AxCrypt (http://www.axantum.com/axcrypt/) is a free, open source product that works with Windows to allow an individual or business to send email attachments in an encrypted format. The person receiving the email needs to know the passphrase to open the file, and this should never be sent by email.

Attend the IT Security Summit New Mexico: On May 3, Santa Fe Community College hosts a one-day security summit where anyone from IT and information assurance professionals to business professionals and entrepreneurs can learn about the latest computer security trends, network with peers and share remediation strategies. Industry experts in research, business, academia, law enforcement and government will address cyberthreats, and a panel discussion called "Virtualization Strategies: A Security Perspective" features chief information officers and IT security professionals from the University of New Mexico, private industry and Los Alamos National Laboratory discussing the security implications of server consolidation projects. The conference is sponsored by the New Mexico Technology Council (NMTC) and the New Mexico chapters of Information Systems Audit and Control Association (ISACA) and the Information Systems Security Association (ISSA). Because space is limited, people are urged to register at www.fbcinc.com/itssnm.

Learn more about Wired Nation at www.wirednation.com.

Finance New Mexico is a public service initiative to assist individuals and businesses with obtaining skills and funding resources for their business or idea. To learn more, go to www.FinanceNewMexico.org. Sponsored by:


NEW MEXICO
ECONOMIC DEVELOPMENT DEPARTMENT


Northern New Mexico
CONNECT


new mexico manufacturing
MEP extension
partnership


NEW MEXICO
SBIC


MONTGOMERY
& ANDREWS
LAW FIRM


CENTURY BANK
People · Relationships · Community


Accounting &
Consulting Group
Certified Public Accountants


Los Alamos
National Bank
Creating a better way.