

West Seneca Firm Protects Company Data

Friday, August 5, 2011

After establishing his computer forensics and data recovering company in 2006, Michael McCartney's West Seneca based DIGITS LLC has received just two inquiries from business owners concerned that someone was hacking into their phone or email systems.



But in July, the wake of the News Corp phone-hacking scandal, he fielded numerous inquiries that led to four investigations of such espionage.

McCartney said his new clients, “for one reason or another, have good reason to believe their private communication such as emails, cell phones or text messages are being compromised.”

According to McCartney, hackers tap personal devices or emails by deploying malicious software (malware)

that attaches to a computer or cell phone through email.

Information can also be obtained through Web addresses in bodies of emails that, when clicked, crawl the computer for passwords and other personal information.

Information is also stolen when someone physically installs software onto a computer or handheld device, he said.

This happens when units are left unattended. He described how this is done to cell phones at lunch meetings, and that thumb drives can be plugged into and removed from computer to get information quickly when someone's back is turned.

There are safeguards people can use to protect themselves from being victimized. McCartney said they include:

- Visit websites of you cell phone and data providers and frequently change your passwords and features such as parental controls.
- Subscribe to and regularly update anti-virus software and anti-malware subscriptions.

“New malware comes out every day,” McCartney said, “and the bad guys are winning.”

- Check Internet and cell phone preferences to make sure Check Internet and cell phone preferences to make sure you know the security settings of the provider, especially on the Web, where it’s easy to get information about someone to do damage- names, addresses, workplaces.
- Limit access to personal devices, and if the cell phone is not password protected, make it so. Also, frequently change the computer login information using passwords that are more than eight characters in length and that combine numbers and letters.