

Westshore Alliance Safety & Security Committee Update

Security Threats Are 'Getting Down to Business' Tips for Keeping your Business Safe (information provided by City of Tampa Police Department)

Internet criminals are increasingly operating like successful businesses, borrowing the best strategies from legitimate companies and collaborating in partnerships with each other to profit from their illegal activities.

According to an influential report released by security analysts, more companies are coming under attack from business-aware criminals who are creating spam around major news events, such as swine flu, to gain access to company systems or persuade victims to visit malware-laden websites.

Social nets questioned...Social networking sites also came under fire in the report. The problem with sites such as Facebook and LinkedIn is that they create an environment of trust among users, who generally assume that links and downloadable content at the sites are always safe. Nothing could be further from the truth, of course.

The recession and the threat of job losses, meanwhile, has led to a rise in disaffected workers who are much more likely to compromise corporate data.

Analysts point out that in addition to using their technical skills to cast a wide net and avoid detection, the new-generation of cyber criminals are also demonstrating some strong business acumen. For example, they are collaborating with each other, preying on individuals' greatest fears and interests, and increasingly making use of legitimate Internet tools like search engines and the software-as-a-service model.

For businesses, experts say the defense strategy is clear: organizations need to adopt ever more advanced ways to fight cyber crime and remain vigilant across all attack vectors.

Social engineers rely on deceiving you in order to commit their crimes. So how do you avoid these traps?

Here are some expert tips to help you keep your wits about you - and your company's data secure:

- Take control of the conversation. One way social engineers gain the upper hand is to seem in charge through conversation. For example, the person who asks the questions controls the conversation; when someone asks

you a question, it immediately puts you on defense. You feel a social pressure to give a correct or appropriate response. If a stranger, perhaps claiming to be from IT support, begins asking you confusing questions about logins and passwords, you must take control. Ask who he is, his extension, his boss, etc. If he's a social engineer, he'll melt away immediately.

- Social engineers take advantage of people's reticence to challenge strangers. For example, this is how hackers walk right through doors for which they lack access cards. If a stranger tries to "tailgate" you this way, politely but firmly insist on escorting them to the nearest security point or their destination.
- Scammers love to capitalize on the natural tendency of most people to help others. A typical social-engineer request often starts out along these lines: "I hate to inconvenience you by asking this, but my boss is going to be upset with me if I don't log in right now and send her ..." Your duty is to make sure company information stays secure, even if this person gets in trouble.