CRN Canada

How to avoid social engineering attacks

by Robert Dutt

The sarcastic note on many a support-desk call ticket reads “problem exists between keyboard and chair.” This universal euphemism for “it’s all the user’s fault” may be true in tech support, but it’s also a growing a problem for security managers. As the technology gets harder to break, attackers are turning to the weakest link in the human-data-computer relationship. And according to Steve Riley, senior security strategist for trustworthy computing at Microsoft, that’s the human.

Organizations spend a huge amount of money, time and thought into securing their network. But “when a human walks along and puts their fingers on the keyboard. It just all goes to hell, and then the human walks away, unaware of what has happened,” Riley said Wednesday at the SecTor security conference in Toronto.

Social engineering is the simple-enough idea of manipulating others to do what you want them to do. It ranges from spam that purports to be from your bank hoping to get you to enter your password, to scammers trying to impersonate the vice president of finance for major international organizations, again trying to steal users’ passwords.

“It works because there is no computer system on Earth that does no rely on humans,” Riley told attendees. “It works because it bypasses every type of technical control and goes after the weakest link.”

It’s much the same as working a scam or a con – to succeed in it, all you have to have is a phone number, and a “mark” from whom you can get valuable information or even hints at that information.

There are a variety of reasons why people fall for social engineering. Maybe they are proud of their knowledge and want to share it, and will say too much to an interested listener. Maybe they’re easily backed into a corner and are judged by the number of calls they complete in a day, so they’re anxious to make callers happy and shut them up. Maybe they just want to help.

The only way to deal with it is with a multi-level defense, based on policy and education, and coming from the C-level executives on down.

But please, not just any policy, Riley urged. If you have a policy that requires users to have unique passwords for all systems, that those passwords be long and complex, and that the users not write those passwords down, don’t be surprised when users utterly ignore the policy.

“We have to face the fact that security is a barrier to progress,” Riley said. “It gets in the way, and it does so intentionally.”

Education is the core of a program to avoid being socially engineered – security is not, after all, an instinctive behavior, and can often be counter-instinctive. Make sure employees know the policy, know the reason behind the policy, and teach them to evaluate risk and expect the unexpected.

“Get this training out a tiny bit at a time,” Riley said. “Make sure it’s attention-getting, and that it appeals to the target audience.”

That education includes learning to effectively communicate to business decision makers they way they understand. If you need a new firewall, liken it to needing new business processes. There’s a need for it – one customer-driven, one security situation-driven – and there’s a cost for both. “If you can speak in the language of the people whose money you want to spend, you’ll go far,” Riley said.