

Security 102

Security Predictions People Still Weakest Link

If one thing is sure not to change in 2009, it's the fact that attackers will likely be using more social engineering methods than ever before -and more socially-driven technologies than ever before- to find their prey.

Why is this fact so certain?

Well, that's easy, because, even if someone can technically **exploit the entire underlying system of trust** (SSL Certificates) on which Web security is built, or, on the flip side, even if our technological protections from attack are stronger and smarter than ever before, the truth remains that the *most significant risk for any computer's security is the person sitting in a chair in front of it, and this will never change.*

Will the person look at the SSL info even if it is there and accurate?

Even worse, as we continue to grow even more dependent on technologies to do things like communicate with our colleagues and friends, we actually become even more prone to exposing ourselves to **external threats**, in particular those that play on our familiarity and comfort in using these tools.

Try **Facebook**, join Twitter, use Skype.

The more we embrace the technologies, the greater the risk of social engineering becomes. And hey, **e-mail scams** still work fantastically well if socially-engineered, a good decade after their invention.

We've been saying this for years of course, but 2008 saw significantly more angles on social engineering - from **threats** carried out on social networking sites like Facebook to greater instances of targeted spear-phishing - than we've ever seen before.

Why? Because people are easy to **fool!** Far more so than computers, and maybe even more so than ever before, it would seem, which is pretty scary to anyone who follows vulnerability research.

So, it's not surprising to see that Trend Micro researchers are finding fake **classmates.com**

invitations being used to suck people into downloading malware.

Or that experts at TrendLabs have found a **ZLOB variant** in rotation among users of Friendster, which still has a massive following in the Far East.

"Since early November we have been observing the increasing occurrence of social networking malware, whose main objective is to trick users into clicking a link which... scores much on credibility, because it often arrives via messages sent through social networking sites' internal messaging functionality," Trend researchers said in a summary.

At the end of the day, IT security, and especially Web security, will only be as intelligent as we, the end users, can be.

And at present, it would seem that, relatively speaking, we're still plenty dumb.

But isn't that why scams have always worked?

SecurityWatchBlog@gmail.com.