Social Engineering vs IT Security: The Bad Guys Don't Fight Fair

When beloved comedian Robin Williams died, most of the world mourned — but not all. While most people suffered pain and loss, a small group of cybercriminals smelled opportunity. And they acted fast.

Within hours of Williams' death, emails were landing in inboxes around the world. "Williams says goodbye…," the emails claimed, inviting people to click a link to view a goodbye video that Williams recorded just before his death.

But there was no video. It was a scam designed to fool people into doing something they wouldn't normally do. It worked.

It's called social engineering. And it's *very* effective.

If They Can't *Hack* You, They'll *Fool* You

Most companies have erected elaborate defenses to protect systems and data from cybercriminals such as hackers. Hackers still have plenty of success, as news headlines regularly report. Many companies, though, have been at least somewhat successful in plugging the types of security gaps that hackers might exploit.

But as a rather strange old saying counsels, there are many ways to skin a cat. And if a direct attack upon your cyber-defenses won't work, cybercriminals can turn to an alternate cat-skinning methodology: social engineering.

Social engineering is not new; it has been around for a very long time. Throughout human history con artists have preyed upon victims, manipulating them into taking actions they wouldn't normally take, or giving up information they would customarily hold secret.

The modern version of social engineering is the same old game. But in the Information Age, the psychological, deceptive sleight-of-hand is often performed with bits and bytes. That form of cyber-attack is far more difficult to defend than a straight-on hacking attempt. And that's why cybercriminals are doubling-down on social engineering efforts.

In fact, ComputerWeekly.com reported that in 2015, social engineering became the top technique used by cybercriminals to thwart cybersecurity defenses.

Same Game; New Names

Through the ages, con men and grifters have relied upon a variety of techniques for fleecing the unsuspecting. The same holds true in the Information Age.

The following are among the most popular and successful of modern social engineering techniques:

- **Phishing / Spear Phishing:** This social engineering technique utilizes email in convincing people to take a certain action or reveal some private information
- **Ransomware:** Victims are duped into installing software that encrypts and locks enterprise data, which remains locked until/unless a ransom is payed
- **Business Email Compromise (BEC) Scams:** Similar to phishing, BEC scams are emails that appear to originate from a high-ranking authority figure, such as a CEO, and that typically direct an employee to transfer funds to an illicit account (This technique is responsible for billions in stolen funds, according to FraudWatch International.)
- **Pretexting:** Often used to impersonate friends, associates or authority figures in soliciting private information
- **Water-Holing:** Malicious code is hidden within popular websites, luring victims to click on links that then infect the victim's computer — particularly effective since visitors to popular sites typically trust that any links within the site are safe
- **Baiting:** Criminals leave some form of data storage media (flash drives, CD-ROM disks, etc.) in a public location, hoping that the curious or greedy will grab and pop them into their computer — whereupon their computer becomes infected with malicious code

Targeting the Good and the Not-So-Good

Technology evolves at lighting speed. But human nature is eternally unchanged. Targeting the foibles of human nature — greed, insecurity, fear — has always led to success for criminals, and always will.

But social engineers also target humanity's *positive* traits. A Sans Institute Report, Methods for Understanding and Reducing Social Engineering Attacks, reveals four key human characteristics that are valued by society, *and* that are specifically targeted by social engineers:

1. Trustworthiness
2. Loyalty
3. Helpfulness
4. Obedience to authority

The unchanging nature of human vulnerabilities assures that social engineers will always have plenty of targets — and also makes social engineering threats particularly difficult to counter.

Stay Alert or Get Hurt

How can you avoid falling prey to a social engineer? The United States Computer Emergency Readiness Team offers a number of tips for protecting yourself and your organization.

Technology can certainly help. Maintaining current versions of the best technological defenses — firewalls, anti-virus software, email filters, etc. — will provide a certain degree of protection.

But technology, by itself, cannot fully prevent the exploitation of human vulnerabilities. The best defense against such exploitation is found in staying alert, and staying suspicious. Regard every email you receive with suspicion; carefully scrutinize every link you consider clicking.

Social engineering attempts range in effectiveness from incredibly clumsy to astoundingly sophisticated. But they all have just one purpose in mind: to turn someone like you into a victim. Don't cooperate.

Summary:

Con men. Grifters. Criminals that prey upon human vulnerabilities have been around forever. These days, those criminal activities are called social engineering. And social engineers have been quick to adapt the latest technology in their quest to find and exploit victims. In fact, social engineering techniques such as phishing and ransomware are now cybercriminals' most popular form of attack.