U.S. Risk, LLC

CYBER INSURANCE: SOCIAL ENGINEERING

Different than technical hacking, social engineering is designed to manipulate people into making mistakes that compromise personal or organizational assets or security through sharing information, downloading software, visiting websites, and sending money to criminals. Often, social engineering strategies are used as the first stage of a larger scale attack.

How Social Engineering Works

Social engineering tactics and techniques are grounded in the science of human motivation. They manipulate victims' emotions and instincts in ways proven to drive people to take actions that are not in their best interests. The primary avenues for social engineering are:

POSING AS A TRUSTED BRAND

INDUCING A FEAR OR SENSE OF URGENCY

APPEALING TO GREED

POSING AS A GOVERNMENT AGENCY/AUTHORITY FIGURE

APPEALING TO HELPFULNESS OR CURIOSITY

TYPES OF SOCIAL ENGINEERING ATTACKS

While every day brings a new way to prey on victims through social engineering, here are some of the top techniques used:

› Phishing

Phishing attacks are one of the most common causes of data breaches designed to gain trust by imitating an organization's identity. Phishing consists of messages that try to manipulate recipients into accessing a website in order to share sensitive information, download malicious software, transfer money or other damaging actions. These messages are crafted to appear from a trusted or credible source. There are many types of phishing, including:

- *Angler phishing uses fake social accounts to masquerade as an official account of a company.*
- *Bulk phishing emails typically appear to be sent by large, well known organizations making generic requests – "please update your credit information."*
- *Search engine fishing is the creation of malicious websites that rank high in Google search for popular search terms.*
- *Smishing/SMS phishing is phishing using text messaging.*
- *Spear phishing, inc. whaling attacks and Business Email Compromise (BEC), typically target privileged access users, using sourced information to craft a message appearing to come from someone known and trusted. Whaling references targeted high profile individuals such as a CEO or a political figure. In BEC, the hacker uses compromised credentials to send email messages.*

- *Vishing/Voice phishing is phishing using phone calls. The most well known is when individuals receive threatening recorded calls claiming to be from the FBI.*

› Baiting

The Nigerian Prince scam is the best-known example of baiting and is an example of victims knowingly or unwittingly giving up sensitive information, or downloading malicious code, by baiting them with an offer they can't refuse. Free software, music, and game downloads infected with malware are other common examples.

› Pretexting

Every social engineering attack involves some sort of pretexting. A suspicious message is received asking for verification of personal information. A request comes in from a high-profile person asking the recipient to do something urgently. Scammers using this method create a fake identity to influence their targets to divulge sensitive information. Often the scammer claims the victim has been impacted by a security breach and will offer to fix things if the victim provides important account information or control over the victim's computer or device.

› Quid Pro Quo

Fake contest winners, loyalty rewards – in a quid pro quo scam, hackers set up a good or service as a reward for the victim's sensitive information.

CYBER INSURANCE: SOCIAL ENGINEERING

› Scareware

It's not only flattery that is used to manipulate, but it can also be fear. Scareware often takes the form of a fake law enforcement notice or fake tech support message using fear to manipulate people into downloading malware or sharing confidential information.

› Tailgating

This technique can be both physical and digital. It can be when an employee is followed into an organization through an unlocked door. It can also be when someone leaves a computer unattended while logged into a private account or network.

› Watering Hole

These attacks involve downloading or launching malicious code from a legitimate website and are aimed at a target, sometimes lying in wait for months before the actual attack. Typically performed by highly skilled hackers, there usually aren't any warning signs. The SolarWinds attack, one of the most sophisticated cyber attacks in history, led to more than 18,000 users downloading tainted software.

THE BOTTOM LINE

Today's cyber threats continue to grow and evolve with insurers holding companies accountable for their cybersecurity programs and controls. A trusted expert highly experienced in cyber policy wording and how to customize policy terms needs to be brought into the process as early as possible to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.