Don’t let hackers fool you with these tricks

Posted on October 11, 2018 by Salena Ferguson

By EDITOR | Published: SEPTEMBER 25, 2018

The volume of malicious cyber attacks is increasing every year. Although many companies use the latest network security systems, they aren’t immune to the hackers’ favorite strategy — social engineering. Unlike malware, social engineering tricks people into volunteering sensitive data. Here’s what you should know to protect your business.

Phishing

This is the most frequently used social engineering attack, especially against small businesses. Check out these frightening statistics:

- Kaspersky Labs revealed that its anti-phishing system prevented more than 107 million attempts to connect users to malicious websites in just one quarter of 2018.
- Barkly added that 85% of companies have fallen prey to this nefarious scheme.

How is phishing carried out? Criminals make use of emails, phone calls, or text messages to steal money. Victims are directed to phony websites or hotlines and are tricked into giving away sensitive information like names, addresses, login information, social security, and credit card numbers.

To protect yourself, be wary of emails from people you don’t know that offer you a prize, come with attachments you didn’t request, direct you to suspicious sites, or urge you to act quickly. Phishing emails usually appear to come from reliable sources, but they are wolves in sheep’s clothing.

One of the most infamous and widespread examples of phishing was during the 2016 Summer Olympics in Rio, where victims received fraudulent emails for fake ticketing services that stole their personal and financial information.

Tailgating

What's the fastest and easiest way for criminals to enter a secure office? Through the front door, of course! Tailgating happens when an employee holds the door open for strangers and unauthorized visitors, allowing them to infiltrate an organization. This simple act of kindness enables fraudsters to enter restricted areas, access computers when no one is looking, or leave behind devices for snooping.

Quid pro quo

Here, scam artists offer a free service or a prize in exchange for information. They may lure their victims with a gift, concert tickets, a T-shirt, or early access to a popular game in exchange for login credentials, account details, passwords, and other important information. Or hackers may volunteer to fix their victims' IT problems to get what they want. In most cases, the gift is a cheap trinket or the tickets are fake, but damages from stolen information are all too real.

Pretexting

Fraudsters pretend to be someone else to steal information. They may pose as a telemarketer, tech support representative, co-worker, or police officer to fish out credit card information, bank account details, usernames, and passwords. The con artist may even convince the unsuspecting victim to apply for a loan over the phone to get more details from the victim. By gaining the person's trust, the scammer can fool anyone into divulging company secrets.

In spite of the many security measures available today, fraudsters and their social engineering schemes continue to haunt and harm many businesses. Thus, it's best to prepare for the worst. To protect sensitive information, educate yourself and be careful. Remember: If anything is too good to be true, it probably is!