the NetWork

LeadingIT

Chicagoland CybersecurITy Support

May 2021

How Human Behavior
Sets Off Social Engineering

Enterprises' Spending on Cybersecurity To
Increase by 20% in 2021

Why You Should Be Worried
About Nation-State 2.0

GoLeadingIT.com (815) 496-6300 @leadingit @leadingit-solutions

How Human Behavior Sets Off Social Engineering

Social engineering refers to any form of manipulation that deceives someone into giving up personal information. Social engineering is also a wide range of malicious activities accomplished through human interactions. To carry out social engineering, an attacker first studies theirtarget and identifies the weak spots. The attacker then gains your trust and convinces you to reveal sensitive information. A reliable IT support team can help you detect some of these breaches early.

Six Techniques Cybercriminals Employ for Social Engineering

1. Phishing

Phishing is the most significant cybersecurity risk that the IT industry faces. Phishing attacks are carried out through email and text campaigns that create a sense of urgency, panic, and fear, prompting the victim to act fast and reveal sensitive information. The emails and texts involve opening links to malicious websites or opening infected attachments. Spear phishing is a more targeted version of phishing aimed at specific individuals. Due to its nature, it requires more effort and has better success rates if well executed.

2. Baiting

Baiting exploits your natural curiosity and makes you expose yourself to an attacker. Baiting involves attracting users into a trap that infects their system or steals their personal information. Placing physical media such as USB drives in places that most people frequently visit offers someone the best condition to pick up the drive containing malware. Baiting isn't only limited to physical media and takes the form of enticing ads and emails offering gifts.

3. Pretexting

This technique relies on lies and tricks. The attacker pretends to need sensitive information from you to perform a critical task. The attacker often impersonates a person in authority and pretends to ask questions that confirm a person's identity. Pretexting forms the basis for identity thefts and secondary attacks. Pretexting works on trust, while phishing works on fear.

4. Tailgating

Tailgating involves the attacker physically following an authorized person into a restricted area. Attackers disguise themselves as delivery guys or strike a conversation with you while passing the screening points. Once inside, they have access to critical technology such as servers.

5. Quid Pro Quo

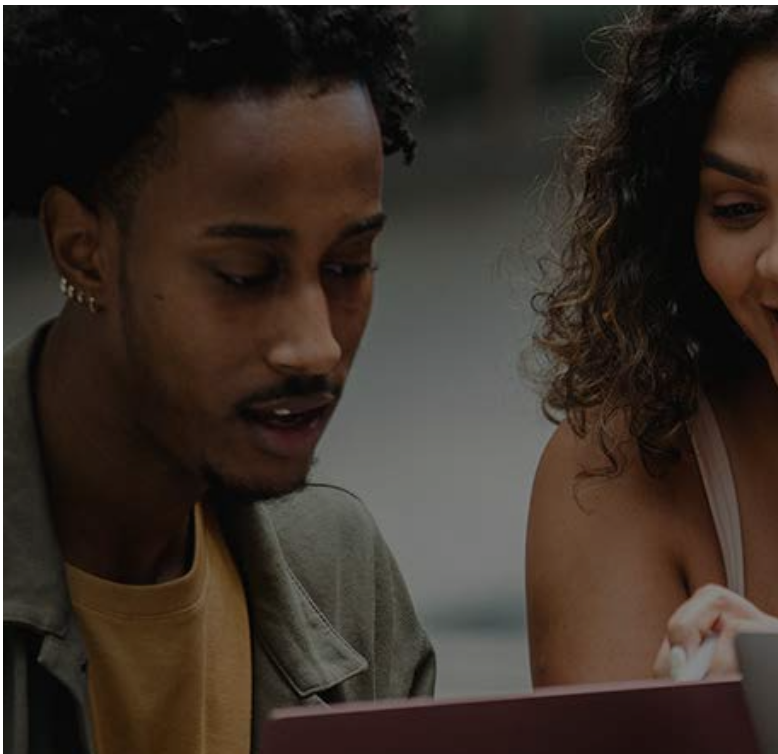
A quid pro quo promises a benefit in exchange for information. Quidpro quo attacks take the form of giveaways and offers that expose you. The reward provided often seems valuable in comparison to the information that you are offering. It is immediately after that you realize there's no reward and your data has already been taken.

6. Scareware

Scareware comes in numerous false alarms and threats, giving you the illusion that your computer is infected. The threats come with an option prompting you to download software that claims to destroy the threat. The software downloaded is malicious software loaded with malware. According to a report by the Washington Post, in 2019, Office Depot and Support.com had to pay $35 million in settlement charges after deceiving customers into downloading a “free PC Healthcheck Program.” Spam mail serves as another way scareware makes way to you by dumping many warnings in our inbox.

Cybersecurity Measures to Help You Prevent Social Engineering

• Train Your Employees. Creating awareness among your employees reduces the risks of them falling bait to an attack. IT services can help create awareness by instructing them on what to do after receiving strange emails or when someone is tailgating them.
• Testing. Performing mock social engineering attacks gauges your organization's response to such attacks. Testing thus helps you identify the breaches in your security protocols.
• Enable Multifactor Authentication. Multifactor authentication safeguards your user credentials and keeps phishing attacks at bay.
• Be Careful of Tempting Offers. Always countercheck when an offer sounds too good to be true. Perform research on the internet to verify the authenticity of the offer.
• Don't Open Email and Attachments from Malicious Sources.



Always countercheck the origin of anything you receive on the internet. If it's from a person you know, but the tone feels off, you can always confirm first through other means such as a telephone. Spam filtering reduces the number of malicious emails reaching your inbox.

• Keep Your Antivirus Software Updated. Antivirus software is usually improved from time to time to cater to emerging cyber threats, requiring constant updating.

• Lock Your Laptop. Whenever you step away from your workstation, always ensure your computer is locked to prevent attackers from planting malware or recovering malicious information.

• Read Your Company's Policy. It helps you understand the circumstances under which you can let a person into the company's building.

• Use Strong Passwords. The passwords you use should be unique and complex. Use a password manager to manage the various custom passwords you use.

• Scan for Data Exposures. Always scan for data exposures and leaked credentials from time to time since it is difficult to determine when a phisher acquired credentials from your organization.

Enterprises' Spending on Cybersecurity To Increase by 20% in 2021

Cybercrime is nothing new in the business environment. Over the years, there have been numerous reports of companies falling victim to hacks. These hacks have resulted in the loss of confidential data, being locked out of their systems, loss of money and business, being sued by clients, disruption of business, and in worst-case scenarios, complete business shutdown.

Why are Businesses Increasingly Investing in their Cybersecurity?

At the onset of the pandemic, cybercriminals changed tactics. They capitalized on the uncertainty and fear brought about by the pandemic. According to a survey by Deloitte, 25% of employees reported an increase in fraudulent messages, phishing attempts, or fraudulent emails on their corporate emails during this time. As a result, Cyberchrology reported that 80% of companies believed that their increased cybersecurity risk during the pandemic resulted from human error.

2020 Named the "Worst Year on Record" in Terms of the Total Number of Records Exposed

According to a RiskBased Security report, by the end of September 2020, about 36 billion records had been exposed. This was more than twice the records exposed in 2019. The FBI reported that cybercrime has increased by 300% since the beginning of the pandemic.

With cyberattack cases constantly on the rise and new, innovative, sophisticated, and lethal methods to get access to your data being formulated and implemented daily, the only safe option for your business is to invest in proactive and robust cybersecurity controls.

It's Time To Rethink Cybersecurity as a Strategic Business Priority

According to Statista, in 2018, the global spending on cybersecurity was around $40.8 billion. Before the pandemic, this figure was expected to eclipse 43 billion US dollars by 2020. With the adoption of remote working by many organizations, the demand for cloud-computing technology and remote working technology to facilitate a safe and confidential working environment has heightened the need for improved cybersecurity.

How Much Should You Invest in Your Cybersecurity?

The short answer is, it depends. How much you pay for your cybersecurity will depend on the type and level of technology you want, the kind of expertise you are looking for, the number of devices you have, and many other factors. started investing in your online security, it's about time you got started. The first step is finding a cybersecurity expert.

Why You Should Be Worried About Nation-State 2.0

Every cyber-security-conscious business leader must recognize the heightened threat levels from nation-state warfare attacks and proactively plan to avert them. Here's why.

Cyber-warfare has been a headache for IT experts since time immemorial, and it seems to be getting more severe by the day. To help us understand this better, let's look at the history of nation-state cyber events.

History Of Nation-State Cyber Attacks

The first nation-state cyber hack to be recorded is probably Clifford Stoll's The Cuckoo's Egg. In this book, he accounts for his hunt for a cyberattacker who broke into Lawrence Berkeley National Laboratory's computers in 1986. It was not until the 1990s and 2000s that cyberwarfare became a real threat. However, even then, established nation-state hacker groups like Maze, Red Storm, Moonlight, and Titan Rain only orchestrated harmless spying operations. The Stuxnet Computer Worm, first discovered in 2010, was a game-changer. Most experts believe that it marked the beginning of Nation-State 2.0. Created by multi-nation-state cooperation, Stuxnet was modular in design and capable of causing physical damage. The initial plan was to use it to obliterate physical nuclear weapon infrastructure. However, it has since been deduced that it triggered more physical damage than a conventional explosive bombing would have done. That's partly because the targets were located in bomb-resistant underground bunkers.

What Is Nation-State 2.0?

Here's what makes nation-state cyber hacks Nation-State 2.0 and why you should be concerned:

1. They No Longer Have Specific Targets: The most startling distinguishing factor is that nation-state 2.0 attacks are spontaneous and untargeted. Nation-state threat actors didn't just attack any organization and without any solid reason. This pattern began changing in the 1990s. According to CBS News, today, any company is a potential target. You can see this in the Microsoft Exchange hack that affected thousands of organizations from almost every industry. Which types of organizations did the SolarWinds hackers target? Nearly all of them. Nation-state attackers no longer discriminate; your organization (and any other) can be their next target.

2. The Threat Actors No Longer Care To Hide: Nation-state hackers used to take their time planning onslaughts to ensure they aren't tracked or noticed. Well, it turns out that's no longer their priority. What does this trend mean for your Chicagoland business? One, if you fall victim, you risk grave reputational dates. You never know what details the hackers may decide to divulge. And two, threat actors are shifting focus from hiding their identities to launching more intricate attacks.

3. Nation-State Hackers Are Now Coming After Your Money: Today, most nation-state hacker groups are going after financial gains. From compromising bank systems and siphoning millions, stealing cryptos, encrypting files, and demanding ransom, nation-state cyber attacking is now a lucrative business. I am persuaded to believe that this is how some nations generate revenue to fund their operations.

What Can You Do To Stay Safe?

- **Include Nation-State Hack Scenarios in Your Risk Modeling:** Now that you know that every organization is a potential target, you should proactively plan to avert such hacks.
- **Monitor Your Systems for Malicious Activities 24/7:** Besides having a system that notifies you if anything foreign invades your network, you should have human eyes on your system round-the-clock.
- **Train Your Staff on Nation-State Attacks, how to identify one, and fast-response protocols.** They're your first line of defense. Nation-state hacks are becoming more brazen, wider spread, more frequent, and with the potential of causing far-reaching damages. The only way to be safe is to assume you're the next target and preparing accordingly.

WE ARE CELEBRATING!

Happy Birthday!

Laura Piekos - May 21st

Read Our Blog For More
https://www.goleadingit.com/blog