SIM2K
Adapting Technology to Your Business Needs

4•22
Information you can use

SIMformation

Phishing Tricks People Still Fall For

Unfortunately, people appear to be lowering their guard when it comes to detecting social engineering tricks. Attackers were more successful last year as more than 80% of organizations suffered a successful e-mail-based phishing attack in 2021, according to a survey of 3,500 professionals. That's a 46% jump from 2020. A study by Stanford University found that about 88% of all data breaches are caused by an employee mistake. Nearly half of employees (45%) cited distraction as the top reason for falling for a phishing scam, and 57% of remote workers admit they are more distracted when working from home. The top reasons for clicking on phishing e-mails are the perceived legitimacy of the e-mail, or that it appeared to have come from a senior executive or a well-known brand.

The consequences of a breach caused by human error are bigger than ever. Researchers identified nearly 15 million phishing messages in 2021 with malware payloads that have been directly linked to later-stage ransomware. And the average total cost of recovery from a ransomware attack reached $1.85 million in 2021, according to Sophos. Why do employees still fall for the same old tricks? One security expert dubbed them the "seven deadly social engineering vices" which most employees still share: Curiosity, courtesy, gullibility, greed, thoughtlessness, shyness and apathy.

5 old social engineering tricks

1. Official-looking email

Employees get an e-mail that appears to come from the company's CEO with the subject line, "You've been mentioned in this document" and the e-mail contains a link titled, "Employee Raises and Promotions 2022." In attempts like these, the bad guys are trying to phish credentials, by making you to log in again with your Office 365 credentials.

2. "Here's a free USB stick"

The FBI warned U.S. businesses in January about fake letters sent through the Postal Service and UPS that impersonated the Department of Health and Human Services offering COVID-19 information, and Amazon in others. Both included a USB stick laced with malicious software. If inserted into a computer, the USB stick could have given the hacking group access to an organization's network to deploy ransomware, the FBI said.

3. The office gift card scam

An e-mail appears to come from an executive at the company asking for assistance to "reward" employees. The goal is to get the person to purchase the cards, scratch off the silver coating covering the codes, then e-mail back a photo of the backs of the cards.

4. "You have a voicemail"

Malware-laced internal voicemails sent through e-mails have resurfaced in recent months. The effectiveness of this depends on who is on the receiving end and their department. A security expert says "An engineer won't check voicemail, but if it's for sales, where that voicemail might be an order, it will be opened."

5. "There's a problem with your package delivery"

Fake parcel delivery notices have flourished for more than 15 years. These phishing attempts come in many variations but are designed to have you login with your e-mail to track a package

4 new social engineering gotchas

1. "Here are your legal documents from DocuSign"

A popular social engineering trick, especially since the beginning of the COVID-19 pandemic, is malware disguised as a request to sign legal documents via DocuSign. The mail will prompt you to install some sort of plugin, which is really computer malware, to proceed with viewing the purported document.

2. The "aging accounts report" scam

In this scam, an employee gets an e-mail claiming to be from a company executive. The message asks the recipient to "please send our latest AR aging report" with a list of all customers who owe money and the amount of time past due. Next, the bad actors create and register a lookalike domain name and they hit up everybody on that list citing how much is owed and when it's owed, and will then say, "We're only accepting ACH payments to this account number going forward." Unfortunately because all information matches, the customers go along. The scam is particularly dangerous because the damage isn't to your company, but to all your customers.

3. "There's a problem with your bank account. Click here to resolve the issue"

Cybercriminals are attempting to convince a target that there is a problem with some high-value account. The e-mail contains a link that will help resolve the urgent issue, which launches a web browser window, taking them to a login page for that account. The victim then enters their credentials, receives the expected message requesting an MFA code, which the victim also enters. The victim sees nothing wrong in the account, but the bad guy now has all the information he needs to loot the account.

4. Phishing by phone

Newer scams use the telephone. Malware impersonates brands like Amazon to convince you that you are being charged hundreds of dollars for a subscription. If you want to cancel, you need to call and speak to a representative. The criminals operate real call centers where they instruct you over the phone how to download the malware and run it on your computer. Other variations of this include similar lures to cancel streaming video services or magazines.

SIM2K urges you to be alert for scams, and call us for help in training employees how to detect and evade such ploys.

SEC Sets Cybersecurity Rules

During its examinations of advisers and funds, the Securities and Exchange Commission has observed a lack of cyber preparedness, determining that existing rules and regulations are likely insufficient to protect clients and investors. Although the Investment Advisers Act already requires registrants to adopt policies and procedures reasonably designed to address applicable risks, cybersecurity risk management is not specifically mandated under current rules. In February the SEC voted to propose new rules designed to enhance cybersecurity practices among advisers and funds, and to increase the effectiveness of cybersecurity-related disclosures to clients and investors.

As proposed, the new Cybersecurity Risk Management Rules can be distilled to four essential components applicable to both investment advisers and investment funds. Under the proposed rules, advisers and funds would be required to:

1. Adopt and implement a written cybersecurity risk management program that includes 5 enumerated components:
- Periodic risk assessment and inventory
- User Security and Access
- Information Protection
- Threat and Vulnerability Management, and
- Incident Response and Recovery.

2. Conduct a formal review, at least annually, of the design and effectiveness of their cybersecurity policies and procedures and prepare a written report. The report should note, among other things, the review process, types of cyber testing conducted, results of such cyber testing, any cyber incidents occurring since the last review, and any material changes to policies and procedures.

3. Disclose cybersecurity risks publicly on regulatory disclosure forms. All advisers would need to describe (1) cyber risks that could materially affect the adviser's services, and how the firm assesses, prioritizes, and addresses these cybersecurity risks, and (2) a description of any cyber incident that has occurred within the last two fiscal years that has "significantly disrupted or degraded" the firm's critical operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm to the firm or its clients. Specific information describing each such incident would be required.

4. Report, confidentially to the SEC, "significant cybersecurity incidents affecting the adviser, or its fund or private fund clients."

The SEC's notes that 58% of financial firms self-acknowledge that they currently underspend on cybersecurity, while recognizing that financial services are arguably the most attacked industry and that remediation costs for incidents can be costly. The SEC realizes that increased costs of compliance with this new rule will be passed on to clients and investors. The costs include increased costs to firms who will need to enhance their cyber programs to align with best practices and with the rule provisions, as well as increased costs to service providers who would be asked for more information and documentation as a result of these rules.

How Strong is MFA?

Multifactor authentication (MFA) is a core defense that is among the most effective at preventing account takeovers. In addition to requiring that users provide a username and password, MFA ensures they must also use an additional factor – be it a fingerprint, physical security key, or one-time password –before they can access an account.

Some forms of MFA are stronger than others, and recent events show that these weaker forms aren't much of a hurdle for some hackers to clear. In the past few months, the Lapsus$ data extortion gang and elite Russian-state threat actors have successfully defeated the protection.

Older, weaker forms of MFA are vulnerable. They include one-time passwords sent through SMS or generated by mobile apps like Google Authenticator or push prompts sent to a mobile device. When someone is logging in with a valid password, they also must either enter the one-time password into a field on the sign-in screen or push a button displayed on the screen of their phone. It's this last form of authentication that recent reports say is being bypassed.

Many MFA providers allow for users to accept a phone app push notification or to receive a phone call and press a key as a second factor. The threat actor took advantage of this and issued multiple MFA requests to the end user's legitimate device until the user accepted the authentication, allowing the threat actor to eventually gain access to the account. There is no limit to the number of requests that can be made, "harassing" the user until they accept the request to quiet the stream of messages. This has been dubbed "MFA Bombing" by security experts.

Newer, more robust forms of MFA aren't susceptible to the technique, as they utilize fingerprint or facial recognition tied to the physical machine someone is using when logging in to a site. In other words, the authentication must be performed on the device that is logging in. It can't happen on one device to give access to a different device.

Organizations must have contingencies in place to deal with these unavoidable events. Many will fall back to more vulnerable forms of MFA in the event that an employee loses the key or device required to send the additional factor.

Any form of MFA is better than no use of MFA. If SMS-delivered one-time passwords are all that's available – as fallible and distasteful as they may be – the system is still infinitely better than having no MFA. But it's clear that MFA on its own is not enough, and it hardly constitutes a box that organizations can check and be done with it. People are beginning to recognize the importance of using MFA correctly. MFA prompt bombing may not be new, but it's no longer something that companies can ignore.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

SMISHING ... Watch your Texts

There's an old adage about finding true love, "There are plenty of fish in the sea!" In the digital world of cyber hacking, they're known as "phish," a scamming tactic used to trick people into revealing confidential information about their bank account, credit card, or other personal accounts. These phishing attempts first started out as phone calls and emails, but now cybercriminals can also reach you via SMS (text message) through a popular phishing scam dubbed "smishing."

A good general rule of thumb for a text from someone you don't know is to just ignore it or delete it, according to security experts. Blocking is an option if you're getting messages from the same source all the time, but the smarter criminals will rotate the numbers they come from. Some tricks to watch out for include:

Scammers act like someone who appears to know you and lure you in with a friendly message. The message may look like this: Beautiful weekend coming up. Wanna go out? Sophie gave me your number. Check out my profile here: [URL]. Smishing attempts try to use common names like Don or Ann that aren't too obvious or hard to pronounce because they want to maintain their not-so-suspicious facade.

Getting a text message saying that you have a package waiting for you, like. " [Name], we came across a parcel/package from [a recent month] pending for you. Kindly claim ownership and confirm for delivery here," and then a link. Clicking on the link and inputting personal information potentially allows cybercriminals to steal your identity.

Hackers disguise themselves as trusted institutions like your bank or utility company to sway you into giving up your password, PIN, or other personal credentials. The message may read something like: "Dear customer, Bank of America is closing your bank account. Please confirm your PIN at [URL] to keep your account activated." Messages of this nature also contain urgent language such as "If you don't reply within 24 hours, your account will be closed." Rather, go directly to the company that is purporting to send you this message. It may require a call to your bank, but at least you'll have confirmation from the source that your personal credentials are safe. Nobody wants to run into problems with their bank. That's why when you receive a text alerting you that your debit card is locked due to suspicious activity, it's very tempting to click the link the text provides to solve the problem – which is exactly what you shouldn't do. "Don't reply to an email, phone call or text message that requires you to give your personal or account information either directly in the email or on a website the email sends you to," says Chase on their website.

An additional precautionary step to safeguard your phone is to install a reputable app or software that's made for mobile device protection. One example is ESET Mobile Security for Android, which has an anti-phishing feature that prevents you from clicking on links within a message that are malicious. A product like this is a good layer of security to have in case you are tempted to click, or the scam looks so legit that you don't even think twice and intuitively click.

"Random Tid-Bytes"

Russian Military Hackers Taken Down

The Federal Bureau of Investigation wrested control of thousands of routers and firewall appliances away from Russian military hackers by hijacking the very same devices Moscow's spies had been using to set up a "botnet" – a network of hacked computers that can bombard other servers with rogue traffic. The operation copied and removed malware from firewall devices that Sandworm used for command-and-control of the botnet. While the operation did not access the Sandworm malware on the underlying victim devices, the disabling of the command-and-control mechanism severed the bots from the Sandworm devices' control, disrupting the Russian military hacker operation. The malware involved, Cyclops Blink, targets network devices manufactured by WatchGuard Technologies Inc. and ASUSTek Computer Inc. While the FBI operation succeeded in copying and removing the malware from all remaining identified command-and-control devices and prevented Sandworm from accessing these devices, WatchGuard and ASUS devices that acted as bots may remain vulnerable to Sandworm if device owners do not take the WatchGuard and ASUS recommended detection and remediation steps, DOJ warned. The department urged network defenders and device owners to review the department's Feb. 23 advisory and the guidance documents that WatchGuard and ASUS released.

UPS Devices now a Target

Hackers have begun to attack internet-connected universal power supply devices, targeting their control interfaces via multiple remote code execution vulnerabilities and, in some cases, unchanged default usernames and passwords, according to an advisory from the U.S. Cybersecurity and Infrastructure Security Agency (CISA). UPS devices, in recent years, have received IoT upgrades – the idea being to allow users to control them remotely via the internet. However, like many other IoT devices, some UPSs have serious flaws in their security and authentication systems, which attackers have exploited to gain illicit access to them. CISA's guidance in the advisory is to immediately take inventory of all UPS devices in use at a given organization, and disconnect them from the internet completely, if at all possible. If they must remain connected to the internet, the agency urged that several steps be taken to mitigate possible compromises, including placing the vulnerable devices behind a VPN, enforcing multifactor authentication, and auditing usernames and passwords to ensure that they're not still factory-default or otherwise easily guessed or cracked.

Europe Enacts New Regulations

Members of the European Union have confirmed the rules that will make up the new Digital Markets Act (DMA). The legislation is intended to rein in the power of large tech corporations such as Apple, Amazon, Google and Meta, forcing them to change how they integrate digital services and handle customer data. To date, any concerns around antitrust has been dealt with by the EU on a case-by-case basis. This legislation is intended to reform the system and address what are seen as systematic issues that exist within the market.

The ABCs of Cybersecurity

Let's be honest, the cybersecurity marketplace is complex and confusing. To help you make sense of today's complex security landscape, our security partner Huntress Labs has defined the key acronyms and capabilities that can be found in several of today's most important security categories.

AV (Antivirus): Antivirus is a type of software that is designed to prevent, search for, detect and remove viruses and other malware from a computer, and is typically installed on the endpoint to block malicious software from infecting the machine, mobile device or network. It works by scanning a file, program or application and comparing a specific set of code with information stored in its database. If the software finds code that is identical or similar to a piece of known malware in the database, that code is deemed malicious and is quarantined or removed.

DLP (Data Loss Prevention): A set of policies, practices and tools used to ensure that sensitive data is not lost, misused or accessed by unauthorized users. DLP solutions provide visibility into who is accessing data and systems (and from where) and filter data streams to restrict suspicious or unidentified activity. DLP solutions are usually deployed as a way to reduce the risk of sensitive data leaking outside an organization, and some solutions can also go beyond simple monitoring and detection to provide alerts, enforce encryption and isolate data as needed.

EDR (Endpoint Detection and Response): An integrated endpoint security solution designed to detect, investigate and respond to cyber threats. EDR solutions offer greater visibility into what's happening on endpoints by recording granular endpoint activity and monitoring for signs of malicious behavior. If the EDR technology detects any of these malicious signs, it will provide security analysts with the necessary information to conduct threat investigations and minimize the impact of an attack.

Firewall: A type of network security system that monitors traffic to or from a network. A firewall acts as an outer barrier that either allows or blocks network traffic based on a predefined set of rules. It scans specific data packets for malicious code or known threats. Should a data packet be flagged, the firewall prevents it from entering the network.

IDS (Intrusion Detection System): A form of network security that uses known intrusion signatures to detect and analyze both inbound and outbound network traffic for abnormal activities. An IDS focuses on monitoring for malicious intent or signs of compromise, and when detected, will send alerts to the system administrators or security personnel. Intrusion detection systems are designed to warn of suspicious activity taking place but they don't prevent it.

IPS (Intrusion Prevention System): A form of network security that can identify malicious activity, collect information about said activity, report it and attempt to block or stop it. Similar to an IDS, intrusion prevention systems are also designed to warn of suspicious activity, but the key difference is that they can also take automated action and respond to active threats based on a predetermined set of rules.

MDR (Managed Detection and Response): A combination of technology and human expertise that tightly focuses on detecting, analyzing and responding to the threats that have snuck past preventive tools. MDR technology collects and analyzes information from logs, events, networks, endpoints and user behavior. A team of experts then takes over to validate incidents, escalate critical events and provide recommended response actions so threats can be quickly remediated. MDR services are managed or co-managed by an outside partner to provide value to organizations that either have limited resources or expertise.

MFA (Multi-Factor Authentication): An authentication method that requires users to provide two or more verification factors before granting access or signing in. These factors can include something only the user would know (e.g., password/PIN); would have (e.g., token); or something the user is (e.g., biometric). MFA then uses these factors to confirm the identity of someone.

NDR (Network Detection and Response): An integrated network security solution designed to detect threats and suspicious behavior on an organization's networks using non-signature-based techniques (such as machine learning and other analytical techniques). NDR solutions track traffic to establish a baseline of normal behavior and raise alerts when anomalous behavior is detected. NDR solutions give security teams real-time visibility and awareness.

NGAV (Next-Generation Antivirus): An expanded version of antivirus that goes beyond performing signature-based detection to prevent a wider range of attacks. Next-generation AV focuses on events (files, processes, applications, network connections, etc.) to help identify malicious intent or activity. NGAV has emerged in recent years to address the proliferation of new types of malware and viruses that can easily bypass traditional AV.

Password Manager: A tool that allows users to store, generate and manage their passwords for local applications and online services. A password manager will house a user's passwords, as well as other information, in one convenient location with one master password. Also, it can assist in generating and retrieving complex passwords.

SIEM (Security Information and Event Management): A software solution that aggregates and analyzes activity from many different sources across an entire IT infrastructure. A SIEM gathers immense amounts of data from an entire networked environment, then consolidates and makes that data human accessible. With the data categorized and laid out, SIEM solutions are often used by security operation centers to centralize data for security monitoring and investigate logs and events for incident response.

SOAR (Security Orchestration, Automation and Response): A collection of software solutions and tools that aggregate security intelligence and context from disparate systems, and applies machine intelligence to streamline or automate the threat detection and response process. SOAR combines three software capabilities: the management of threats and vulnerabilities (orchestration), automating security operations (automation) and responding to security incidents (response). Due to its aggregation and automation capabilities, SOAR solutions are often used by security operation centers (SOCs) to collect threat-related data from a range of sources and automate the responses to certain threats.

SOC (Security Operations Center): A centralized unit that deals with security issues on an organizational and technical level. A SOC acts as a central command post that continuously monitors an organization's environments, preventing, detecting, analyzing and responding to cybersecurity incidents.

Threat Hunting: The practice of searching through environments to detect and isolate advanced threats that evade existing security solutions. Threat hunting combines technology, threat intelligence and methodical humans to find and stop malicious activities. Generally, threat hunting is performed by security analysts who use their highly tuned skills to zero in on potential threats or attackers.

XDR (Extended Detection and Response): A security technology that provides extended visibility, analysis, detection and response. XDR solutions access data from multiple sources to detect more advanced attackers and quickly respond to those threats. XDRs are usually comprised of EDRs, NDRs, NGAVs and cloud monitoring tools.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com