White paper

The rise of social engineering and the cost of personal devices: A security perspective

verizon

Introduction

From the innocuous use of personal devices (bring your own device, or BYOD) to social engineering attacks, the cyber threat is all around us, often creeping out of places we least suspect. Not only are these threats becoming more widespread, but dedicated attacks are also more complex and convincing. Even the biggest companies are not immune to the potentially disastrous effects of a sophisticated social engineering attack or device mismanagement.

There is no getting around human weakness.

Many potential weak links and vulnerabilities can be exploited in business settings, whether in microenterprises, medium-sized companies or large corporations. Some weak links require a high level of technical knowledge to detect, making them difficult to protect against attacks. Others, however, are easily exploited and often overlooked, presenting low-hanging fruit for threat actors.

Unfortunately, in the latter case, humans are an ever-present weakness that can be easily exploited, unwittingly exposing enterprises to risks – whether it is by fraudsters targeting them mercilessly with sophisticated scams, such as smishing and robocall attacks, or because employees are simply bypassing security tools to optimize their work. In today's remote/hybrid corporate world, BYOD policies are more widely implemented to boost employee productivity and reduce hardware costs, although both of those reasons may not always hold true in practice. While BYOD may bring these benefits, it also potentially carries a significant cyber risk.

Social engineering: Smarter and more dangerous

With the increasing sophistication of social engineering (and today with the use of artificial intelligence [AI] and deep fakes to create highly convincing voice impersonations), even the savviest users can have difficulty detecting these attack schemes.

Scammers will typically seek out the weakest link in an organization, which often is the human element – such as disgruntled employees, lost personal devices used for work or executives who think they are communicating with someone they know. Wherever your weak link lies, there is a prime opportunity for threat actors to gain access through phishing (email/messaging), vishing (phone/voice) or smishing (text/Short Message Service [SMS]) attacks. For instance, a global ride-sharing company's network was compromised in late 2022 when an attacker targeted a contractor who was using a personal device. After the device was infected with malware, the threat actor bought the contractor's corporate password on the dark web. After repeatedly rejecting multifactor authentication requests, the contractor eventually accepted a request, allowing the threat actor to gain network entry.[1]

As another example, one of the world's largest media and entertainment companies recently had to shut down its computer systems for 10 days[2] after hackers successfully impersonated an employee and convinced the IT help desk to reset the user's password. Just through some basic online research on social media, the hackers seemingly managed to eventually take control of a multibillion-dollar company's computer systems. If these types of attacks and scenarios can happen to global brands with nearly limitless resources, what does that say for midmarket organizations?

With such a high level of network access, threat actors have a great deal of leverage, ready to demand a ransom or go straight to disclosing or selling your sensitive data on the dark web. Breaches of this nature can also significantly damage your brand reputation, translating to potential drops in share prices and the possible alienation of consumers with data privacy concerns.

Corporate usage of personal devices is proving costly.

Enterprises must also contend with the fact that humans have the natural inclination to make their lives as easy as possible, always looking to simplify and streamline operations. This inclination has translated into the growing use of personal devices, which can present a dangerous risk to enterprises as they lose visibility and control not just over business processes but also over corporate security. This risk is not always created maliciously by the employee. Instead, it simply reflects a very human impulse to get things done in a convenient and timely fashion. While there are potential advantages of using personal devices in terms of business productivity, their use can nonetheless compromise the integrity of the work environment. Most worryingly, they can lead to regulatory compliance failures and expose the enterprise to financial liability.

This is similar to what happened recently in several high-profile cases in the U.S. financial services industry, which came to light in 2021. A number of large financial services providers were heavily fined (from US$9 million to more than US$100 million each) by the U.S. Securities and Exchange Commission (SEC) for improper policing of employees' use of off-channel messaging services and for failing to maintain and preserve all official communications by their employees.[3] The fallout was costly, both from a reputation and financial standpoint.

The human risk factor cannot be understated. As so many unfortunate tales making recent news headlines highlight, the digital landscape is fraught with danger and risks. The challenge for enterprises now is to constantly manage both attacks and device misuse while minimizing the potential blast radius on business operations.

1. "Security update," Uber newsroom, September 16, 2022. https://www.uber.com/newsroom/security-update
2. "MGM Resorts computers back up after 10 days as analysts eye effects of casino cyberattacks," The Associated Press, September 21, 2023. https://apnews.com/article/vegas-mgm-resorts-caesars-cyberattack-shutdown-a01b9a2606e58e702b8e872e979040cc
3. "SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures," U.S. Securities and Exchange Commission press release, August 8, 2023. https://www.sec.gov/news/press-release/2023-149

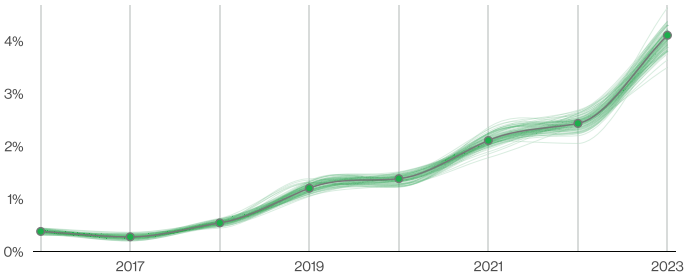
Exploiting low-hanging fruit: People and their devices

From a risk perspective, there is no doubt that some of the low-hanging fruit involves human weaknesses. How are these weaknesses being actively exploited or triggered? Verizon's "2023 Data Breach Investigations Report" (DBIR) outlines some of these threat vectors.

People problems

People include not just employees and executives but also customers and third parties in the supply chain. They can be targeted with spray-and-pray email phishing tactics, but increasingly we are seeing spear phishing (targeting specific individuals), whaling (spear phishing attacks targeted at high-level employees), smishing (phishing attack via text messaging/SMS) and vishing (phishing attack via phone call/voice) attacks deployed as well, with successful outcomes. These types of attacks often require little technical knowledge. Background secondary research on social networks and some inventive scamming are usually more than enough for the threat actor.

- According to the 2023 DBIR, 74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials, or social engineering.
- Business email compromise (BEC) attacks – pretexting attacks where attackers will oftentimes play on an invented scenario – have almost doubled within the past year across the DBIR's entire incident dataset and now represent more than 50% of incidents within the social engineering pattern. Moreover, BEC attacks cost victims US$10.3 billion in losses in 2022, as reported by the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) unit.

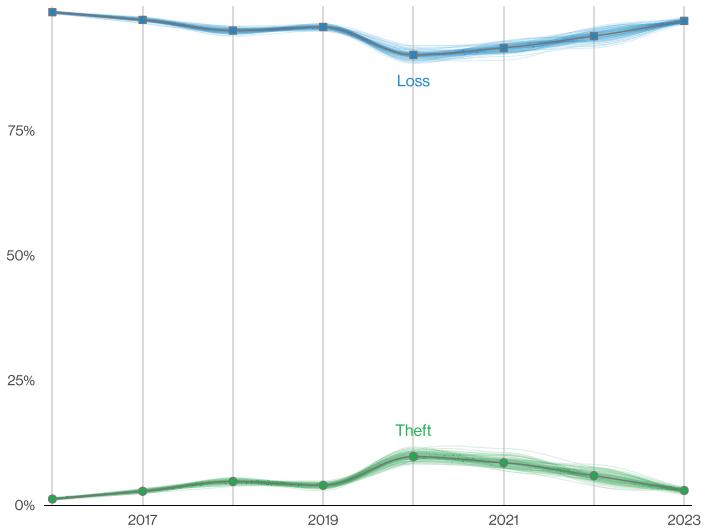


Pretexting incidents over time

Vulnerable technologies

Technologies that may be vulnerable include personal computers, mobile devices, network systems, cloud infrastructure, software and applications. Remote work is here to stay in the post-pandemic world, with 92%[4] of remote workers using their personal devices for work tasks. They also use these devices for entertainment (social media, mobile apps, etc.), posing potential cyber risks. This is a huge challenge for enterprises due to policy and regulatory compliance risks and corporate data leakage. Verizon's Mobile Security Index (MSI) reports that more than 50% of personal devices fell prey to a mobile phishing attack in 2022, with text messaging (SMS) attacks increasing the odds sixfold to tenfold (compared to email phishing attacks). The problem is that these personal devices may be managed by the individual employee, with enterprises having little to no control or visibility over device use. As a result, employees may unknowingly engage with a threat actor, and their company may not be aware of that activity until it is too late.

- While stolen devices (laptops, mobile phones, etc.) certainly represent a risk to organizations, employees are much more likely to cause a breach accidentally through loss.
- 78% of employees use their work devices for personal activities (social media, email, etc.), and nearly half let friends and family use their work devices according to Verizon's MSI. These seemingly harmless decisions can lead to a companywide network breach if devices are not protected and monitored.
- This pattern of employees using work devices for personal activities continues to be a problem for organizations as these small portable devices store more information, but employees continue misplacing them.



Top Action varieties in Lost and Stolen Assets incidents

4. "New Lookout Research Highlights Increased Security Risks Faced by Organizations Due to Remote Work and BYOD," Lookout press release, April 3, 2023. https://www.prnewswire.com/news-releases/new-lookout-research-highlights-increased-security-risks-faced-by-organizations-due-to-remote-work-and-byod-301787467.html

Is BYOD really worth the risk?

It should be noted that some companies are still willing to accept the risks of BYOD. Some choose to allow personally liable devices because they are perceived to improve employee productivity or because they reduce IT spending. However, the cyber risks associated with a lack of control over employee personal devices are a tough pill to swallow.

Another factor to consider is the lack of supply chain management for BYOD and choose your own device (CYOD). As referenced in NIST SP 800-124r2, your employees are potentially using devices that have been rooted, jailbroken with vulnerable apps or even infected with malware without the user knowing.[5] If you cannot pinpoint the origin of your employees' devices, your IT team may already be at a disadvantage. Ultimately, enterprises are paying the price for human weakness and BYOD policies. But the outlook is not hopeless. Plenty of security technologies can be implemented, and Verizon is one provider working hard to mature, evolve and create comprehensive solutions in this space.

5. "Guidelines for Managing the Security of Mobile Devices in the Enterprise," National Institute of Standards and Technology, May 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf

How Verizon is helping

Regulated industries in the crosshairs

Verizon has been working to enhance security for enterprise customers across various sectors. Notable work comes in helping defend organizations in heavily regulated spaces such as financial services that face growing challenges from two fronts: stricter regulatory pressure and increasingly complex social engineering attacks. At a minimum, corporate devices are a requirement for regulated companies. Using personal devices without recordkeeping software carries heavy legal and financial consequences for regulated organizations, as noted earlier.

In the United States alone, more than US$1.5 billion in penalties have been racked up since the SEC started investigating recordkeeping tactics at financial institutions.[6] That includes 16 Wall Street firms that were fined US$1.8 billion for allowing employees to discuss deals and trades on personal devices via text messages/WhatsApp.[7] As useful as mobile device management (MDM) software may be in curbing cyber threats, personal devices still carry significant risks; it's still up to the end user to remember to maintain the security posture.

Corporate devices have security benefits you cannot get with BYOD. Swapping personal devices for corporate-issued ones can allow IT staff to gain a better grip not just on internal/external communications but also on various integrity and security aspects of mobile devices. When organizations offer corporate-liable devices from Verizon, they are gaining enhanced security protections and controls not available on personal devices.

This can help to address common vulnerabilities for organizations. For example, while trying to comply with regulators, many companies are contending with high levels of robocalls. Unfortunately for banks, robocalls have become tougher to detect because threat actors use advanced deep fake technologies to re-create synthetic speeches, allowing them to impersonate banking customers.

Among the Verizon solutions that can be used to counter such attacks are compliant calling, voice authentication and defense solutions, and voice honeypots across its wireless and wireline networks. Voice and text honeypots capture spam calls and texts targeting Verizon customers. We then use artificial intelligence and machine learning (AI/ML) to process the content, looping in human analysis to review and escalate new scam campaigns for mitigation.

Financial services are not the only regulated organizations under intensive attack. Healthcare providers are also being targeted by opportunist social engineers, with fraudsters focusing on employees similarly through smishing and vishing attacks. Third-party, low-quality internet service providers (ISPs) may sometimes provide numbers to threat actors, who subsequently use the numbers to conduct targeted attacks against those employees.

To help counter these attacks, our threat intel team—using its honeypot with thousands of phone numbers—has a high success rate, to date, in investigating and disconnecting fraud-related phone numbers at customers' requests. Moreover, the incident response teams have also been able to shut down suspicious numbers.

Organizations also have the ability to go a step further and take a proactive perspective, as Verizon offers executive protection services. Our threat hunting team can scour the dark web and help remove personally identifiable information (PII)—such as email addresses, phone numbers and physical addresses—about high-level employees that can be used to target them (and their family and social circles) in social engineering attacks.

Implementing a comprehensive defense plan

The first step any business must take in defending its network from social engineering attacks is to understand the nature of the cyber risks being faced. An outline should be created to establish a clear understanding of how to mitigate, minimize, transfer or accept the identified risks. This risk assessment is a critical step because it allows you to identify your assets, threat entities and risk appetite. From there, putting together a comprehensive defense plan becomes much easier because you know what your security goals are and what red flags to look out for.

A defense plan against social engineering attacks comprises two main functions: threat detection and trust enforcement. Both functions apply equally to help detect and counter high-level threats and low-level vulnerabilities.

6. "SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures," U.S. Securities and Exchange Commission press release, August 8, 2023. https://www.sec.gov/news/press-release/2023-149
7. "U.S. fines 16 Wall Street firms $1.8 bln for talking deals, trades on personal apps," Reuters, September 27, 2022. https://www.reuters.com/business/finance/us-fines-16-major-wall-street-firms-11-billion-over-recordkeeping-failures-2022-09-27

How Verizon is helping

Threat detection is a cybersecurity discipline that focuses on identifying and dealing with threats such as cyberattacks, compromises, data breaches and incidents once they occur. This is done by spotting and helping stop unauthorized access, malware, social engineering schemes, etc. Trust enforcement is all about getting out in front of potential attacks by leveraging techniques such as identity management, passwords, encryption, access control, authentication, etc. Both of these functions form the bedrock of a broader defense plan against social engineering attacks that protect networks, applications, devices and identities.

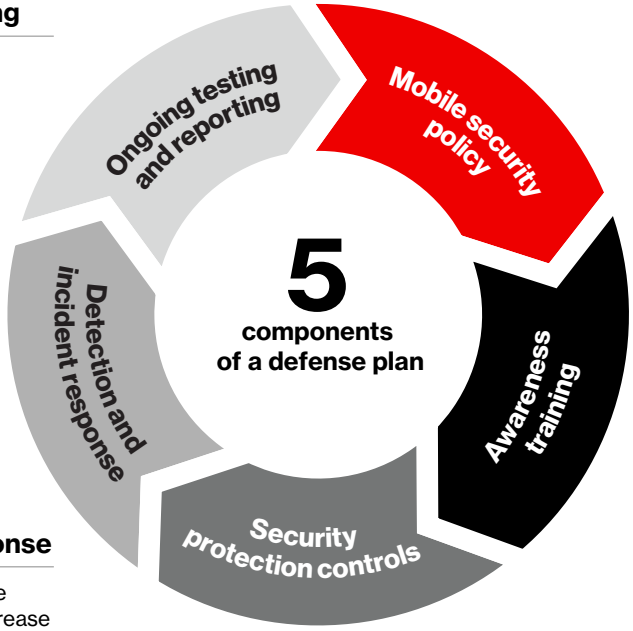
Verizon provides both of these functions in five key areas of control: awareness training, mobile security policy, security protection controls, detection and response, and monitoring and testing across devices, applications, identities and networks.

Social engineering defense plan recommendations

Ongoing testing and reporting

Ensure that you have a team with knowledge of social engineers' tactics and a team that conducts regular security positioning assessments, including:

- Penetration testing
- Tabletop exercises
- Ransomware assessments
- Daily dark web intelligence
- Cyber risk quantification



Mobile security policy

Institute a companywide mobile security policy:

- Consider using corporate-liable devices to help ensure that employees discuss business on business phones
- Maintain consistent policy and protection controls across all devices
- Help support regulatory compliance.
- Support chain of custody and forensics
- Mitigate supply chain risk
- Measure organizational wireless performance

Detection and incident response

Near-real-time detection and response capabilities can be critical to help decrease the effect of cyber incidents, including for you and your third-party vendors:

- Security operations services
- Endpoint and network detection
- Incident response
  - Honeypot reporting and response
  - Investigating and helping block the source causing the incident
  - Forensics data support
  - Executive identity protection

Security protection controls

Controls must be applied at all levels, from device to network, and across all channels, including third parties:

- Email, chat, mobile, Short Message Service (SMS) and voice defense solutions
- Zero-trust and secure service edge architectures
- Identity and access management
- Multifactor authentication (MFA) and FIDO2
- Encryption technologies
- Third-party security access controls

Awareness training

Educating employees, partners and third parties on security red flags (e.g., solicited personal information) and how to protect their devices with virtual private networks (VPNs) and MFA.

Training exercises such as phishing, vishing, smishing and quishing tests that are critical to keep people on alert.

A unique position: Visibility, reach and experience

Security-conscious network providers like Verizon can have an advantage over traditional security vendors with their bird's-eye view of traffic, devices, technologies and users. For all customers, from small business to enterprise, Verizon offers a broad range of solutions including customer reporting, ongoing threat monitoring and sending out advisories. In this regard, every piece of data is ingested, analyzed and then conveyed into actionable insights.

Verizon's customers gain the newfound ability to "see" what was always out of sight. This outlook grants them a high level of visibility across the entire spectrum of assets being used at any given time as well as all the interactions between them. From this bird's-eye view, we provide enterprise customers with comprehensive management, from device to network, on which they can layer vetted security controls. That means they can benefit from inherent security at the network level, such as registered short codes to provide hard-to-spoof identification, texting "off" to 4040 to stop unwanted email-to-text messages, 7726 spam message reporting and filtering, attestation of Voice over Internet Protocol (VoIP) via STIR/SHAKEN, and distributed-denial-of-service (DDoS) protection on the Verizon VoIP network.

At some point, all organizations will require real-time supervisory control over employee devices to help curb increasingly sophisticated cyber threats. Verizon is well prepared to fill this final security gap (keeping in mind that it simply cannot be fully achieved with BYOD devices). We provide both a baseline security package for the entirety of our wireless network and customized security for enterprise clients, either through corporate-liable end-user devices or dedicated security services. We leverages our understanding of the issues involved in migrating away from BYOD policies—such as security challenges, high stipend costs, and complexity in developing separate configurations and applications for personal devices—to assist clients transitioning to corporate lines.

Moreover, Verizon can tailor a custom cybersecurity solution as part of a customer's holistic defense plan against social engineering threats. Ditching BYOD and going with Verizon corporate lines can help provide you with the granular cyber insight needed to properly assess modern social engineering tactics and identify them promptly. With a tailored deployment, we can help enact dedicated protection mechanisms to help keep your assets safe and reduce risks, including deploying security analysts with threat hunting backgrounds to scrutinize customer information on a daily basis as well as identify and respond to suspicious patterns and attacks. As previously alluded to, these outcomes are challenging when your employees use their personal devices.

Beyond this, Verizon can offer a range of solutions that can address trust enforcement and threat detection. But importantly, as noted, it all starts with risk assessment. Our consulting services can help enterprises assess risks and provide advice on security posture, whether these are high-level threats or common, everyday risks.

Verizon's cybersecurity expertise and role as a network provider create the perfect combination to provide a holistic view and comprehensive security strategies for companies. Partnering with us, your organization can have a network that, with the application of key security products and services, can help provide protections against those simple, everyday cyber attacks as well as more complex threats covering people, technologies and processes. Effectively assessing the social engineering risks that your organization's mobile device policy may pose starts with you asking the following questions:

- How would underlying malware or spyware or malfunctions on a personal device, such as a smartphone or tablet, affect visibility, business operations and access to corporate information?
- How will cellular forensics and consent be handled when a personal device is implicated?
- Have we assessed user privacy implications when considering a BYOD vs corporate-liable policy?
- Have we assessed the conditional access controls, their available capabilities and their gaps in a supervised vs BYOD environment?

If you need to learn more about these mobile security threats and how your organization should tackle them, a good starting point is to visit the NIST Mobile Device Security site today.

Verizon is offering a customized five-point social engineering defense plan for businesses. To learn more, contact your account representative or have a specialist contact you. verizon.com/business/contact-us/

verizon