How social engineering scams help spark uptick in cybercrime

ISAAC SARPONG: Isaac is the Partner in charge of Tax Services. He has over 26 years' experience in the provision of multi-faceted advice to both local and international clients in taxation, accountancy, audit & assurance, and corporate law, among others. Isaac is a Chartered Accountant, a Chartered Tax Practitioner and a Lawyer.

EY

Building a better working world

Even digital-savvy Gen Z is vulnerable to being duped

In brief

- Social engineering attacks are rising in the workplace, adding to widespread concerns about escalating cybersecurity threats, according to new data.
- Notably, Gen Z and millennial employees are less confident identifying and responding to cyber threats than their older colleagues.

Social engineering attacks are rising in the workplace, adding to widespread concerns about escalating cybersecurity threats, according to **new data** from Ernst & Young LLP.

Although they are a digital-first generation, Gen Z is losing confidence in its ability to recognize phishing attempts, in which a victim clicks on a malicious link that installs malware, reveals sensitive information or freezes systems as part of a ransomware attack. Only 31% of Gen Z feels confident they can identify phishing attempts, and 72% say they opened an unfamiliar link that seemed suspicious at work, far higher than millennials (51%), Gen X (36%) and baby boomers (26%), according to the **EY 2024 Human Risk in Cybersecurity Survey**, a study of 1,000 employed Americans across public and private sectors.

Social engineering manipulates human psychology, unlike traditional hacking methods that exploit technical vulnerabilities. "Even the most well-funded defenses, where investments in leading cyber technology have been built over years, can fail or be bypassed if an employee is fooled into giving access to a cyber thief," says Jim Guinn, II, EY Americas Cybersecurity Leader. "And it can happen quickly – in just a matter of minutes."

Attackers may pretend to be a distraught fellow employee desperately trying to recover vital information on a lost phone, reset a password or need help wiring money to an account. The intended target wants to help a fellow employee in need. This desire to assist may quickly undermine even the best-laid security plans. A successful cyber attack could disrupt basic operations, compromise customer and company data privacy, threaten a company's reputation and create significant legal and economic consequences. A severe cybersecurity incident at a major resort and gaming giant in 2023, for instance, was facilitated using an IT employee identified on a business and employment-focused social media platform and a 10-minute call to the help desk, according to reports.

"Even the most educated and experienced members of your security staff are vulnerable to social engineering," says Guinn. "These criminals are very, very good at what they do."

Chapter 1

The primary weapon

Three types of social engineering attacks are common:

1. **Phishing:** Phishing emails look trustworthy but link to or contain malicious content that executes as soon as users click it, encrypting their data. That brings a ransomware attack. Spear phishing attacks target a specific person or group. Threat actors have also expanded to "smishing," which is sending malicious text messages that can lead to the recipient authorizing an action or divulging personal information.
2. **Pretexting:** Pretexting involves creating a fabricated scenario that gains a target's trust to extract sensitive information. For example, an attacker might pose as a bank representative and ask for account details under the promise of sending a check.
3. **Baiting:** Baiting involves offering something enticing, such as a free download or prize, to lure victims into clicking on malicious links or downloading malware-infected files. Sometimes, an attacker might claim to be an IT support technician offering assistance and requesting login credentials.

Guinn notes that social engineering attacks often share a common tone. "There is often a sense that time is of the essence in order to keep the victim off-balance," says Guinn. "For instance, it might state that funds are needed today or that someone's job is on the line. The human condition to help can enable good-intentioned employees into becoming victims."

Chapter 2

New attack surfaces

With cloud adoption, attack surfaces have increased exponentially.

During the COVID-19 pandemic, many employees began working from home. Many still do. The heavy reliance on remote electronic communications may cause employees to unduly trust emails and texts. With less face-to-face interaction, and more reliance on electronic communication, there is a feeling among security professionals that a targeted victim may potentially be less vigilant and let their guard down. One result was the increase of malicious emails purporting to be from a colleague.

There is also widespread concern about the role of artificial intelligence (AI), which can deliver disinformation and fraudulent messages at unprecedented scale and sophistication. One example is AI-generated deep fakes, which are synthetic media that creates unsettlingly real videos, pictures, audio and text. They can convincingly mimic a person's voice, face and gestures and are weaponized against companies. According to EY research, 85% of respondents believe AI has made cybersecurity attacks more sophisticated, and 78% are concerned about the use of AI in cyber-attacks.

Through cloud adoption, attack surfaces have also increased exponentially. Services that used to run on big data centers, Guinn notes, are now in the cloud. If those resources are misconfigured, it exposes sensitive information, gives excessive privileges or creates security gaps.

Misconfigurations include improper settings, permissions or access controls, or leaving them at default values.

Cloud misconfiguration can be a force multiplier during a security breach, says Guinn, because "the cloud is a big window to crawl through and it gets an attacker into the good stuff – a company's enterprise systems – very quickly. Then, they're like a fox in a hen house: they start grabbing everything in sight. Once that critical enterprise info is secured, these cloud-based attacks often result in devastating double extortion ransomware attacks." In 2023, according to reports, about 60 credit unions experienced some level of outage due to a ransomware attack at a third-party cloud service provider.

Chapter 3

How to protect your organization

Protective strategies should include the following:

The **EY 2024 Human Risk in Cybersecurity Survey** notes that 53% of respondents are worried their organization will be the target of a cyber attack, and 34% are concerned that their actions may leave their organization vulnerable.

Cybersecurity professionals say a strong security posture must pervade every organization. Position cybersecurity protocols as working in partnership with their employees, not as police, by embracing a fundamental "see something, say something" policy. Make reporting potential attacks and vulnerabilities simple enough for workers to seemingly integrate them into their daily lives.

> "
>
> **When security practices are ingrained in the company culture, employees are more likely to prioritize security in their day-to-day activities and proactively report potential security incidents,**
>
> says Dan Mellen, EY US Cyber Chief Technology Officer.

(CONTINUED IN NEXT EDITION) ■

STRATEGY CONSULTING

EY-Parthenon professionals recognize that CEOs and business leaders are tasked with achieving maximum value for their organizations' stakeholders in this transformative age. We challenge assumptions to design and deliver strategies that help improve profitability and long-term value.

Our purpose is building a better working world. It starts with better questions. The better the question. The better the answer. The better the world works. Please send an email to **isaac.sarpong@gh.ey.com** and copy in **kofi.akuoko@gh.ey.com**

About EY

EY is a global leader in assurance, tax, strategy and transaction and consultancy services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, clients and for our communites.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

Find out more:

Address: 60 Rangoon Lane, Cantonments City, Accra.
P. O. Box KA16009, Airport, Accra, Ghana.
Telephone: +233 302 772001/772091
Email: info@gh.ey.com,
Website: ey.com

How social engineering scams help spark uptick in cybercrime

ISAAC SARPONG: Isaac is the Partner in charge of Tax Services. He has over 26 years' experience in the provision of multi-faceted advice to both local and international clients in taxation, accountancy, audit & assurance, and corporate law, among others. Isaac is a Chartered Accountant, a Chartered Tax Practitioner and a Lawyer.

EY
Building a better working world

Even digital-savvy Gen Z is vulnerable to being duped

Continued from previous edition

Protective strategies should include the following:

1. Stay up to date on cyber threats.

Plan for regular vulnerability assessments that help identify deficiencies in the configurations of information resources and whether attackers can exploit those gaps.EY 2024 Human Risk in Cybersecurity Survey reveals that most respondents (91%) say organizations should regularly update their training to keep pace with AI, especially as AI's role evolves in cyber threats. Still, only 62% of respondents say their employer has prioritized educating employees about responsible AI usage.

2. Upskill your team's cybersecurity skills.

To stay ahead of the evolving security challenges, you'll need an adaptive workforce. Equip the organization with the right skill sets and promote collaboration across sectors – even though it can be challenging. According to the World Economic Forum, there is a global shortage of nearly 4 million cyber professionals, with an estimated 52% of public organizations stating that a lack of resources and skills is their biggest cybersecurity challenge.

3. Drive employee engagement with gamification.

Younger generations are more likely to not fully understand what their organization's process is to report suspected cyber attacks, even though their organization has a set plan in place, according to EY Consulting research. Leaderboards and multiplayer features in gamified training programs encourage healthy employee competition, driving them to perform better.

> “
>
> **Creating a game out of cybersecurity awareness, with incentives like team lunches or extra time off, can significantly increase engagement and knowledge retention,**
>
> says Guinn.

5. Train. Train. Train.

EY Consulting research finds that employees who are "rusty" in cybersecurity training are most fearful of using technology at work. Regular penetration testing allows you to plug the holes in the security of critical information.

6. Use failures as opportunities.

A compromise assessment, for instance, helps identify current and past intrusions into an organization's information and resources. Professionals use tools that analyze information resources to identify indicators of compromise and detect traces of an attacker's activity in the information environment.

> Adequate security is not a **"set it and forget it"** endeavor, Guinn notes. It must be an ingrained and agile part of a company's culture.

> “
>
> **Everyone in a company, no matter what their position or responsibility, is on the front line of cyber defense,**
>
> says Guinn.

> "The risk landscape has become incredibly complex. We are all in this fight. Either we stand as one or we risk falling together."

Summary

Rising social engineering attacks are adding to widespread concerns about escalating cybersecurity threats. Protective strategies are crucial to staying ahead of cyber risks and should include cultivating a culture of confidence, upskilling your team's cybersecurity skills, driving employee engagement with gamification and using failures as opportunities.

CYBERSECURITY, STRATEGY, RISK, COMPLIANCE AND RESILIENCE

EY Cybersecurity, strategy, risk, compliance and resilience teams can provide organizations with a clear picture of their current cyber risk posture and capabilities, giving them an informed view of how, where and why to invest in managing their cyber risks.

Our purpose is building a better working world. It starts with better questions. The better the question. The better the answer. The better the world works. Please send an email to **isaac.sarpong@gh.ey.com** and copy in **kofi.akuoko@gh.ey.com.**

About EY

EY is a global leader in assurance, tax, strategy and transaction and consultancy services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, clients and for our communites.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

Find out more:

Address: 60 Rangoon Lane, Cantonments City, Accra.
P. O. Box KA16009, Airport, Accra, Ghana.
Telephone: +233 302 772001/772091
Email: info@gh.ey.com,
Website: ey.com