proofpoint.

EBOOK

The Security Awareness Handbook

Six essential topics every user should know — and every organisation should teach

Introduction

Today's cyber threats rely on human interaction, not just technical exploits. In fact, 82% of data breached in Verizon's 2022 *Data Breach Investigations Report* involved the human element. As the report puts it, this reality "puts the person square in the center of the security estate."[1]

Attackers use social engineering to trick people into clicking unsafe URLs, opening malicious attachments, entering their credentials, sending sensitive data, transferring funds and more.

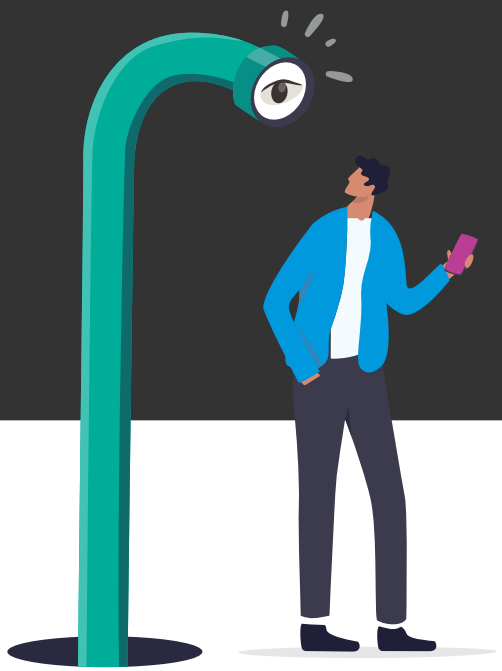
That's why teaching your employees how to thwart cyber threats is critical to the security of your organisation. Threat prevention and detection technologies can't stop every attack. Your people must recognise and be empowered to act when faced with the whole gamut of modern threats.

The volume and variety of attack vectors is limited only by threat actors' creativity. But most of their approaches fall into a handful of categories that rely on the active participation of victims. And the good news: you can equip your users to recognise, reject and report these threats before they cause lasting harm to the organisation.

This e-book covers the risks your users are most likely to face:

- Social engineering
- Phishing
- Business email compromise (BEC)
- Social media
- Ransomware
- Insider risk

We'll dive deep into each threat, exploring the mechanisms of how they work, the damage they can cause and how to keep your users aware and ready for them.



1 Verizon. "2022 Data Breach Investigations Report." June 2022.

Table of Contents

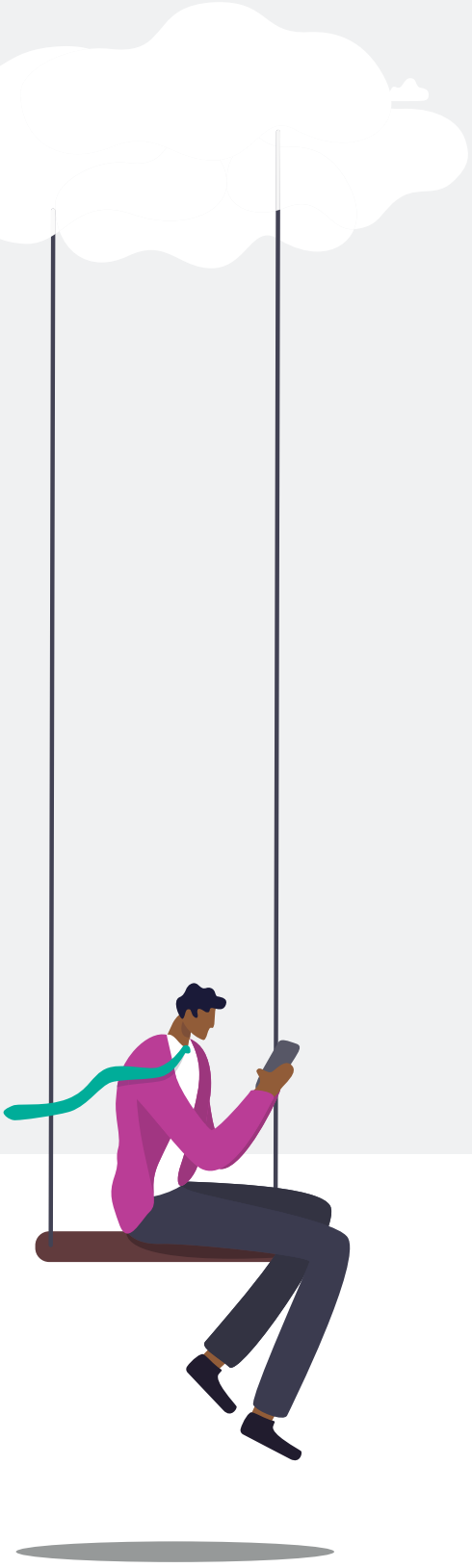
SECTION 1

Social Engineering

The goal of this security awareness programme is to reduce human risk and help build a strong security culture that drives behaviour change.

Users must be motivated and embrace the critical, frontline role they play in helping to protect the organisation. They need to know how attackers manipulate them to enable their campaigns and why they are being targeted. That makes social engineering—which plays a role in almost every human-focused attack—a foundational cybersecurity awareness topic.

Even your savviest users can benefit from reviewing the basics of social engineering as part of their awareness education. So let's start from the top with a definition.



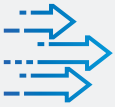
What is social engineering?

Social engineering is a collection of techniques that malicious actors use to manipulate human psychology. It's exploiting human nature to trick or threaten users to take actions such as:

Giving up account credentials

Handing over sensitive data

Running malicious code



Transferring funds

Why do attackers rely heavily on social engineering for so many campaigns? Because they know that people are the easiest way into an environment. (Plus, why do all the dirty work when you can get someone else to do it for you?)

How attackers use social engineering to exploit people

When covering social engineering as part of your cybersecurity awareness, be sure to also discuss *how* attackers exploit users with these techniques. For example, explain that threat actors will take advantage of users':

- **Emotions,** by conveying a sense of urgency, generating excitement about an opportunity or creating fear around losing money or doing something wrong
- **Trust,** by posing as someone the user trusts or abusing a trusted brand or authority (such as the IRS, UPS, Amazon and Microsoft)
- **Fatigue,** by timing attacks when users are likely to be tired or distracted and more inclined to let their "emotional mind" guide their decision-making.

Types of social engineering attacks

Security awareness training on social engineering should review a few common techniques.

Phishing

This method refers to sending malicious emails to trick people into doing something on the attacker's behalf. It usually involves clicking a malicious web link in the email or an email attachment. Research for the "*2022 State of the Phish*" report from Proofpoint shows just how prevalent and effective phishing is: In 2021, 86% of organisations faced bulk phishing attacks. In phishing simulations, 1 in 5 users opened an email attachment, and 1 in 10 clicked on a link.

Social media reconnaissance

Attackers often use social media to gather information about users that they can leverage as part of another campaign. For example, they might gather information from LinkedIn about a company's top executive so they can impersonate that executive in a phishing campaign. Posing as the executive, the attacker might target users in the financial department. Attackers' reconnaissance efforts may also include direct outreach to a target.

Vishing and smishing

With this social engineering technique, attackers use text messages and voice-changing software to send SMS messages to users or robocall them. The messages often promise gifts or services in exchange for payment. These types of scams are called vishing (voice phishing) and smishing (SMS/text phishing). (Check out our blog to dig deeper on the differences between vishing and smishing.)

Telephone-oriented attack

As we explain in our *2022 Human Factor* report, telephone-oriented attacks—also known as callback phishing—have surged in recent months. These attacks often start with email and play out over multiple channels. But the linchpin of this approach is a person-to-person phone conversation.

Naturally, these attacks require the victim's active participation. Telephone-oriented attacks start with an email that claims to be from a legitimate source and includes a phone number for customer assistance. Callers are connected to fake customer service representatives. These "representatives" then navigate the victim through the attack. They may instruct the victim to let them access their machine remotely or download a file that turns out to be malware.

What to teach your users

Wrap up your social engineering training with some tips that your users can start putting into action right away. Here are some recommendations to share with your users:

- Never blindly trust anyone who contacts you by email, phone or social media.
- Slow down and think twice before taking any action—such as carrying out a request to send money or buy gift cards without confirming the sender (and the request itself) is legitimate.
- Never share personal information, such as phone numbers or home addresses, in social media posts.
- Be cautious about clicking on links and opening attachments. And never give anyone your credentials.
- Common sense can go a long way toward preventing a social engineering attack. If it seems too good to be true, it's very likely a scam. And if something doesn't look or sound right, it probably isn't.

SECTION 2

Phishing

Phishing has been around for decades but remains one of today's biggest—and fastest growing—cyber threats.

Already a growing challenge before the COVID-19 pandemic, phishing activity has only gotten worse since then. According to the latest annual *Internet Crime Report* from the FBI's Internet Crime Complaint Center (IC3) losses from internet-related fraud, which usually involves some kind of phishing, rose nearly 50% in 2022 to $10.3 billion. And those numbers reflect only reported phishing attacks; the true number is likely far higher.

By any measure, cyber attackers are clearly succeeding in their efforts to exploit human vulnerabilities. Yet research for the *2023 State of the Phish* report from Proofpoint found that only 58% of working adults know what phishing is.

The message for organisations: Phishing needs to be a focal point of your security awareness programme. If it's likely that only about half of your users know what phishing is, consider leading off your education about this crucial cybersecurity awareness topic with an explanation of the term.

What is phishing?

Phishing is an example of social engineering, which is a collection of techniques—including forgery, misdirection and lying—that attackers employ to manipulate human psychology.

Phishing emails use social engineering to encourage users to act quickly, without thinking things through. And when attackers succeed in tricking users with phishing messages, the rewards can include access to sensitive data, critical systems and networks, cloud accounts and often money.

Most phishing messages are sent by email. But some attackers deliver these messages to victims through other methods, including smishing and vishing (using text messages and voice-changing software to send SMS messages to users or robocall them).

Three primary threats in phishing messages

Once your users have a better understanding of what phishing means, outline some of the typical strategies attackers use to compromise the recipients of phishing messages.

Malicious links

Attackers often use malicious URLs in phishing messages. When users click on a malicious link, it may take them to an impostor website or a site infected with malware (malicious software). Often, attackers will carefully disguise these links in phishing messages so that they appear to be from trusted sources. Techniques may include using company logos or registering email domains that are confusingly similar to those of a trusted brand or business.

And all too often, the attacker succeeds. Our research for the *2023 State of the Phish* report shows that more than 1 in 10 users will click on a malicious link in phishing simulations.

Infected attachments

Attachments infected with malware can compromise computers and files, and they often look like legitimate file attachments. In phishing simulations we conducted for customers, we've observed that 16% users will open an email attachment.

It's important to explain to users the harm phishing can cause. Malware infections and ransomware delivered through a phishing attack can easily spread across networked devices—and even to cloud systems.

Fraudulent requests

These requests are designed to convince the email recipient to return sensitive information, such as login credentials, credit card information and more. They are often presented as a form (for example, from a tax authority promising a refund) to prompt the user to provide sensitive information.

Once the user fills out and submits the form, malicious actors can use that data for their personal gain.

All phishing attacks use social engineering

As noted earlier, phishing attacks are a form of social engineering. In your security awareness training, you'll want to draw attention to some of the ways that attackers take advantage of human psychology to manipulate users, such as by:

- Masquerading as someone or something the user would likely know and trust
- Taking advantage of emotions such as fear (or even just stoking the fear of missing out) to motivate users to act quickly
- Making exciting promises that sound too good to be true (and definitely are)

Also, malicious actors will often try to time their attacks for when a user is likely to have their guard down, such as when they're feeling tired or distracted. Many attackers will also study a company's billing cycle or learn when important meetings are held before they launch a phishing attack.

The bottom-line impacts of phishing for businesses

As part of your end-user security awareness programme, you may want to point to a few significant incidents to help underscore just how costly phishing attacks can be for businesses. This information can be especially compelling for senior executives. Because of their access and authority, they are among the types of users most often targeted or impersonated by attackers in phishing campaigns.

Here are some real-world examples:

- **In a proposed settlement** over a massive 2021 data breach, a mobile telecommunications company in the United States has agreed to pay out $350 million to customers whose data was allegedly exposed. The incident affected more than 76 million customers.[2]
- An executive of sportswear giant Nike **lost an estimated $173,000** in digital tokens in a January 2023 in what he called a "clever" phishing attack. "Obviously pretty upset and hurt by this," the executive wrote in a tweet. "I [haven't] really been able to move all day."[3]
- A phishing attack tricked a Mailchimp employee into handing over credentials, which cyber criminals then used to steal account data for nearly 320 customers and more than 100 marketing email lists. Adding insult to injury, the attacker went on to launch additional phishing attacks designed to appear as if they came from Mailchimp itself.[4]
- Two leading technology companies in the United States—one a social media platform and the other an internet search engine—lost more than $100 million in an elaborate phishing scheme. Attackers went as far as setting up a false company and using fake emails and invoices.[5]

What to teach your users

Of course, for cybersecurity awareness training to resonate with users, they need to understand how phishing schemes can potentially erode their bottom line, too. Help your users learn to be on the lookout for phishing tactics involving:

- Online shopping (such as "Click here to order now, and you'll get 60% off! Plus, you'll be entered to win a free $1,000 shopping spree on our website.")
- Charities (such as "Help fight hunger this holiday season—the need is extremely urgent. Please use this form to donate what you can right now.")
- Shipping providers (such as "We could not deliver your item. Please review the attached shipping information to confirm your order details.")

Also, alert your users to the potential for "streaming scams," where attackers pose as legitimate providers of popular streaming services, offering special deals (maybe "One month free!") or try to convince users they need to take action on their account (such as "Update your details to reactivate your membership").

2 Jonathan Stempel and Sara Merken (Reuters). "T-Mobile to pay $350 mln in settlement over massive hacking." July 2022.

3 Matthew Kish (Insider). "A Nike exec says a phisher stole his NFTs. Here are 3 things everyone should do to protect a digital wallet." January 2023.

4 Ryan McCurdy (Security Boulevard). "The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023." November 2022.

5 Vanessa Romo (NPR). "Man Pleads Guilty To Phishing Scheme That Fleeced Facebook, Google Of $100 Million." March 2019.

Keep it simple, security leaders

Complete your training on the cybersecurity awareness topic of phishing with some easy-to-implement advice that can help your users avoid falling for a phishing scheme. Here are a few habits that should become instinctive to security-aware users:

- Not trust the sender immediately, even if the message appears to be from a trusted source or brand
- Scrutinise the sender's address—and inspect any links that appear to be from shipping providers (such as "We could not deliver your item. Please review the attached shipping information to confirm your order details.")
- Open a new browser tab or window and manually type the domain that the link appears to be pointing to
- Not click on calls to action within the email, like "verify your account" or "log in now"
- Understand that file-sharing links aren't always safe

And finally, urge your users to report every message that they consider suspicious. Email reporting should be a critical part of your cyber defenses—and tools like the PhishAlarm phishing button make it easy for your users to become vigilant and proactive defenders.

SECTION 3

Business Email Compromise

An accountant wires money to the construction firm renovating a corporate office. A payroll specialist updates banking information for a newly married employee for the week's payroll. These are both ordinary scenes and routine business processes.

They're also the targets of one of the most insidious types of cyber threats, known as business email compromise (BEC). BEC attacks masquerade as routine business email and use the power of familiarity and trust to divert money and information into malicious hands.

BEC attacks rely on social engineering—and human nature—to succeed. It's critical that your users understand what BEC is, how to recognise it and what they can do to stop these attacks.

What is business email compromise?

Business email compromise is a type of email fraud. Criminals impersonate a trusted source using a spoofed, lookalike or compromised account. Then they send targeted emails to employees, business partners or customers. The recipient, believing the email is legitimate, takes actions that place sensitive information or funds directly in the hands of the criminal.

BEC's impact

The impact of BEC is considerable. In 2022, **the FBI reported** that adjusted losses from BEC attacks totaled $2.4 billion. That's 49 times greater than losses from ransomware and represents 35% of all losses reported in 2021. A single diverted wire transfer can easily cost your business hundreds of thousands of dollars or more.

$2.4B

In adjusted losses from BEC attacks

49x

greater than losses from ransomware

of all losses reported in 2021 were from BEC attacks

Common tactics

Here are four main impersonation tactics used in BEC attacks:

- **Domain spoofing:** Attackers take advantage of gaps in your email authentication system—or lack of one—to make it appear that an email is coming from your trusted domain.
- **Display name spoofing:** Attackers modify the sender's name to display someone known to the recipient. Sometimes this a person in authority, but it can be anyone the victim trusts (internal or external).
- **Lookalike domain:** Attackers register domains that are confusingly similar to your company's domain and impersonate the brand or a trusted individual. For example, an attacker might swap acompanysdomain.com for acompanydomain.com.
- **Compromised account(s):** Attackers use various tactics, such as social engineering and phishing to gain access to a user's email credentials. They then use that compromised account to launch BEC attacks. Attackers may also use a compromised account from a trusted vendor to defraud customers and business partners—turning the supply chain into another threat vector. We often see supplier impersonation and compromised supplier accounts used jointly in a single attack.

Common themes

Several themes appear frequently in the content of BEC messages. All aim to get users to complete a task or provide information.

- **Lures and tasks.** Attackers use simple, seemingly benign questions or requests to identify, verify and soften up potential targets. They may seek to dig up more information, confirm that the email address is valid or see whether the target seems easy prey.
- **Payroll redirect.** Attackers send an email to HR or payroll department posing as an employee and ask to change their direct deposit banking information. This change routes your employee's pay to the bad actor's account.
- **Invoicing fraud.** An attacker impersonates or compromises an internal source or a supplier and requests that payments be routed to a new account.
- **Extortion.** Extortion-themed email fraud works like other forms of extortion. The attacker threatens to destroy property, commit violence or release confidential, embarrassing or compromising information unless the recipient provides payment (typically through cryptocurrency) or something else of value.
- **Gift carding.** In gift carding schemes, threat actors obtain payouts in the form of retail gift cards. Recipients are tricked into buying the cards and sending the numbers and PINs to the attacker, who then redeems or resells the cards.
- **Advance-fee fraud.** Advance fee fraud is an old con that is sometimes, and somewhat misleadingly, called "419," "Nigerian 419" or "Nigerian prince" email fraud. It occurs when a threat actor asks the potential victim for a small amount of money in advance of a larger payout later. The requested funds are usually depicted as seed money to unlock or transfer the promised reward.

Meet-and-cheat: BEC in the age of Zoom

With the rise of remote work, virtual meetings have become a common theme in BEC attacks. Attackers use this technology theme in several ways, such as:

- Sending meeting invitations and citing "audio issues" at the start of the meeting; then using in-meeting chat or follow-up emails to request money or information
- Using "deep-fake" audio or video to impersonate someone the victim trusts
- Impersonating a company leader who's "stuck in a meeting" and asking staff to complete finance-related tasks
- Using a compromised employee email account to gain access to sensitive information, get employees' schedules and slip into ongoing email conversations

Whatever the method employed, users must be able to recognise BEC attempts that exploit remote and hybrid work.

What to teach your users

BEC attacks are difficult to spot because they look just like regular business emails. They don't always contain URLs or attachments, making them hard to detect with traditional security tools. But your users can look out for signals that something is awry and take steps to verify requests. These steps can include contacting the sender in person or through a different communication channel, such as the telephone.

- **Misspellings:** While they are not a smoking gun, misspellings should prompt your users to take a closer look at the email and ensure the request is valid.
- **Sudden change in procedures:** Emails that ask for sudden changes to procedures—and especially those involving finances or private company data—should always be treated with suspicion.
- **Banking or financial requests:** Employees should always scrutinise requests to change banking or payroll information.
- **Urgency:** Any sense of urgency should also raise a red flag for your employees. Attackers use urgency to elicit an emotional response from their recipient.
- **Hover over sender display name:** Closely look at the sender email address to see if it's a lookalike domain. When users reply to an email, always check to see if the reply-to email is consistent with the email in the sender field.

Employees can help your company combat BEC attacks in several other ways. Share this advice with them:

- Be careful when posting personal information online. Attackers will often research targets to make their impersonation more convincing.
- Don't trust any senders. Always be on the lookout for imposters.
- When in doubt, consult the security team.
- Always verify requests for money or information using other methods to ensure they really came from the apparent sender.

SECTION 4

Social Media

Less than 20 years ago, only 5% of Americans used social media. Today, the figure stands at 72% as platforms like Facebook, Twitter, Instagram, Tik Tok and countless others weave themselves into the fabric of everyday life.[6]

In the process, social media has also become a hotbed for crime. According to the U.S. Federal Trade Commission (FTC), more than 25% of reported fraud in 2021 originated on social media. And the victims are not necessarily who you would expect. It's not just older people who are falling victim to social media fraud; all demographic groups are affected. In fact, the FTC reports that people between the ages of 18 and 39 were more than twice as likely as those over 40 to fall victim to social media scams in 2021.[7]

6 Pew Research Center. "Social Media Use in 2021." April 2017.

7 FTC. "Social media a gold mine for scammers in 2021." January 2022.

Why social media?

Attackers love social media because most people have at least one social media account. Because social media is informal and part of peoples' personal lives, many users lower their defenses when using these platforms. And they often use social media at times when they are tired or distracted, such as in the evenings after work or waiting in line. All of this adds up to make social media an easy target for attackers.

Types of social media attacks

Users of social media may face many types of threats. Attackers typically use several activities to lure users into providing personal information, credentials or money.

Impersonation

Attackers pretend to be someone a user knows or a representative from an institution they trust, such as the Internal Revenue Service or the Social Security Administration.

For example, your employee may receive a message that appears to come from a friend. The friend claims that they are stuck overseas after being robbed. And they need your employee to send money urgently to help them get home.

Or your employee might receive a message from the Social Security Administration saying that they have been trying to contact them and need them to take urgent action (such as clicking on a link to log into your account or confirm their address).

Healthcare fraud

These scams use healthcare topics that are top-of-mind, such as COVID-19 or monkeypox. Users are enticed to click on a link or provide personal information in exchange for:

- Testing kits, which fail to materialise or are fake
- Fake COVID-19 vaccination cards
- Vaccines, treatments and remedies, which are often fake

Attackers will also offer money or gifts in exchange for completing "surveys" about vaccination or treatment. These "surveys" are vehicles for stealing personal data, medical information or financial details.

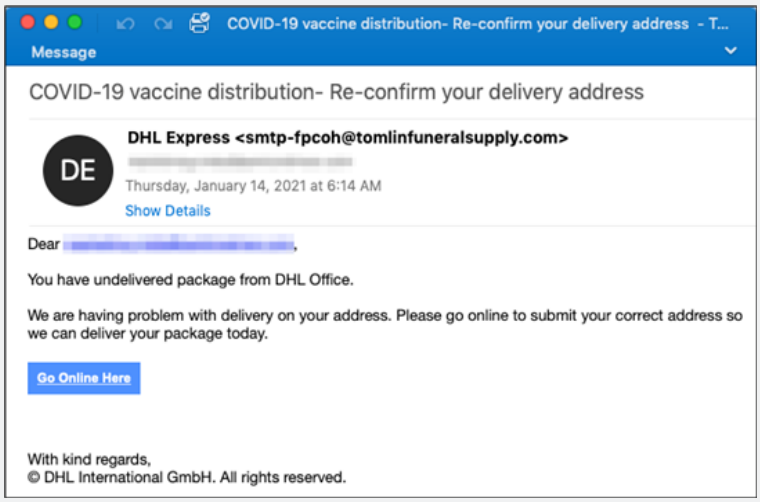


Figure 1: A screenshot of an email purporting to inform the recipient about an undelivered DHL vaccine package.

Clickbait

Clickbait scams lure users to click on malicious links with promises of shocking or embarrassing content. Users may receive a private message (often appearing to come from a trusted friend) that suggests the sender has found a lewd or otherwise compromising photo or video of the recipient.

When the user clicks on the link to view the media, they are prompted to update software required to view it and end up installing malware. Because people will want to quickly get the photo or content removed and experience feelings of embarrassment and potential shame, they are less likely to stop and check if the link that is being sent is safe. This is just one of the many ways that attackers leverage emotions.

Phishing

Social media phishing happens in two main ways.

In the first, attackers send emails that appear to come from a social media platform. The email explains that the user's account password has been compromised. The user is instructed to click on a link to maintain access to their account. This link leads to a fake login page that harvests the user's credentials. This works because attackers have targeted the user's emotions and created a sense of urgency, as the user now feels they have to act fast to restore their social media account to safety.

In the second type of social media phishing attack, users receive friend requests from people they appear to know. These accounts, which are either compromised or faked, post content with malicious URLs that lead to a fake login page. From a social engineering standpoint, the attackers try to exploit people's basic desire to connect and build social, personal relationships with others. This makes it likely that users will be motivated to click on friend requests quickly and without verifying that person's identity.

Romance scams

Romance scams are a form of impersonation scams. In a romance scam, attackers adopt a fake identity to foster a romantic relationship with a user, sometimes over a long period of time. Once trust has been established, they usually manipulate the user into sending money.

In September 2021, a former U.S. Army reservist was sentenced to 46 months in prison for his role in a scheme to swindle more than $1.8 of dollars from nearly 70 victims across the country. The scheme created fake identities to dupe older men and women into believing they were in romantic relationship, then exploiting their emotions to get money from them.

And who hasn't heard of the notorious "Tinder Swindler" (a.k.a. Shimon Hayut, a.k.a. Simon Leviev)? Posing as the playboy son of a diamond tycoon, Hayut showered women with gifts, attention and whirlwind vacations—before asking them for money to fend off mysterious "enemies."

Sweepstakes and lottery scams

Sweepstakes and lottery scams use promises of prize winnings as a lure for users to provide personal or financial information. Attackers know that people will always be interested in winning money, so they hope to appeal to the excitement and joy of an unexpected windfall.

Quizzes and polls

Quizzes and polls that appear in social media feeds may seem like a fun and harmless activity. But attackers often use quiz scams to harvest personal information from users, including answers to common security questions.

Remote work and money-making schemes

These scams are a form of employment fraud. Attackers pretend to be recruiters and lure users with advertisements for high-paying, easy work that can be done from home. These remote-work job scams are merely a front for stealing personal information and money from the users who respond to them.

How these scams can hurt your organisation

Although most of your employees are unlikely to use social media as part of their regular job duties, social media attacks have the potential to harm your company. If an employee's device or accounts become compromised through one of these attacks, it can give attackers a foothold to launch an attack within your company.

In today's remote work environment, people use their personal devices for work and personal life. That means any attack can compromise sensitive information and data from work that can cripple organisations.

What to teach your users

You can help your employees understand how to safely engage with social media by sharing the following tips:

- Always treat requests for money and credentials with extreme suspicion, even if they appear to come from someone you know. If you receive a request for your money or credentials, always contact the person through another channel to verify.
- Beware of promotions, job advertisements and pop-up messages making promises that seem too good to be true.
- Don't enter your username or password into websites unless you have navigated to the site directly and verified the URL in your browser.
- Delete any requests for sensitive data and report them to your security team if you receive them on company accounts.
- Only contact social media support and contacts by navigating to the social media website or app directly.
- Watch out for messages that ask for money urgently, even if they come from someone you know. Always take your time to check in outside of social media with the person making the request.
- If you think your account has been compromised, immediately log in and reset your username or password. If you have trouble, report it to the social media site.
- Don't open social media websites in the same browser window as your banking website or other sensitive sites. Attackers can sometimes capture important information this way.

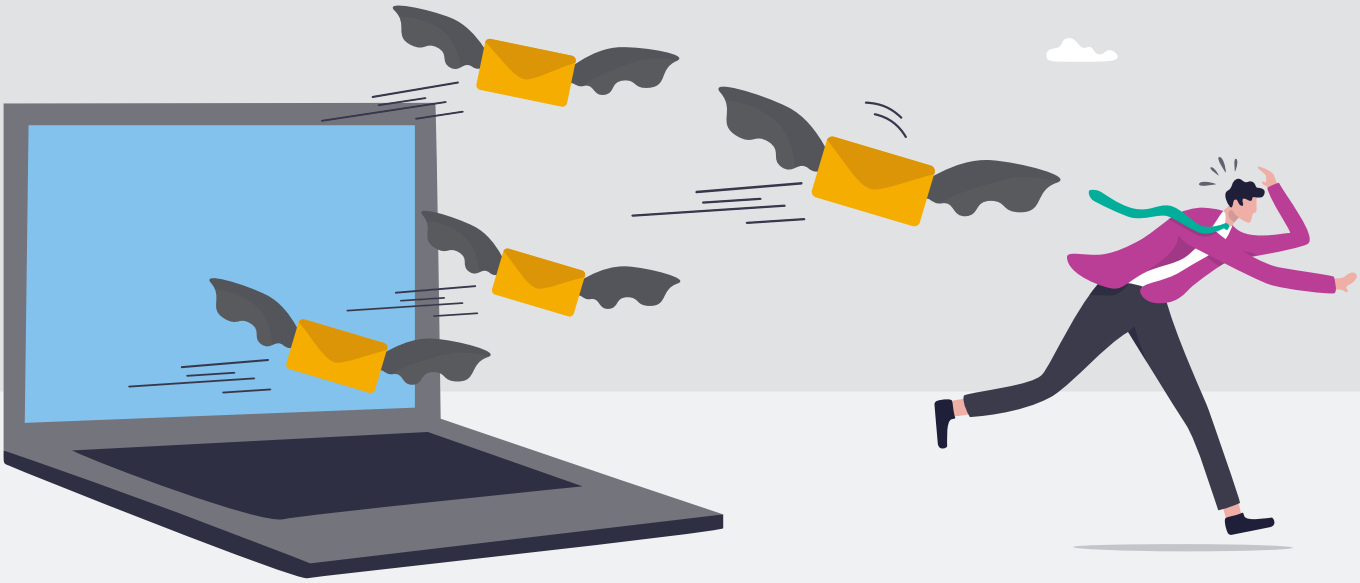
SECTION 5

Ransomware

Ransomware is more than three decades old but remains one of today's most disruptive types of cyber attack.

This category of malware—which gets its name from the payment it demands after locking away victims' files— can be traced back to 1989, when an evolutionary biologist unleashed the "AIDS virus" via floppy disk in a scheme to extort funds from AIDS researchers in 90 countries. Recipients were instructed to mail their payments—which the attacker referred to as "licensing fees"—to a P.O. box in Panama. Once payment was received, a decryption key would be mailed back to the users. The attacker profited little from this escapade and was eventually arrested.

Since then, ransomware attacks have greatly evolved. They are often sophisticated campaigns with far-reaching impacts and multimillion-dollar payouts. Ransomware attacks can also have devastating consequences when they target critical infrastructure and services, like healthcare, law enforcement and energy—as they increasingly do. This threat type is also considered a national security issue, as many attackers are associated with or bankrolled by nation-state threat actors. In fact, victims of ransomware in the United States are encouraged to report ransomware incidents to the U.S. government.



Ransomware attacks have become more prevalent in recent years—likely because of the opportunity for attackers to profit royally from these incidents. Research from Palo Alto Networks Unit 42 found that the average ransom demand rose 144% in 2021 to $2.2 million, and the average payment increased 78% to $541,010.[8]

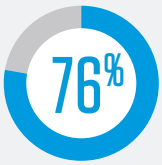
144%

rise in ransom demand in 2021

$541,010

average payment for ransom

And in our own research for the *2023 State of the Phish* report, Proofpoint learned that:



of organisations saw email-based ransomware attacks in 2022

of organisations were infected by ransomware

of infected organisations paid a ransom

1/3 of adult users incorrectly identified ransomware

Ransomware is a costly, disruptive cyber threat that organisations must address in their security awareness programmes. Paying ransoms, while sometimes unavoidable, only encourages attackers to repeat their behaviour—and helps fund the next attack. A better approach is to prevent ransomware from taking hold in the first place. The opportunity to increase user awareness of the ransomware threat is high, given that 40% of adult users assessed by Proofpoint couldn't identify ransomware correctly. (See the results of this assessment in our *2023 State of the Phish report*.)

Research from Unit 42 shows that more than 75% of ransomware is delivered by email and about 20% through web browsing. Ransomware operators often rely on social engineering—and human nature—to compromise users and launch their attacks. It's critical that your users understand what ransomware is, how to recognise it and what actions they can take against these highly disruptive attacks.[9]

8 Ryan Olson (Palo Alto Networks). "Ransomware Trends: Higher Ransom Demands, More Extortion Tactics." March 2022.

9 Ibid.

What is ransomware?

Ransomware is essentially a tool that enables extortion. It's a type of malicious software (malware) that locks away critical data, usually by encrypting it, until the victim pays a ransom to the attacker.

Ransomware infections can occur when a user unknowingly downloads the malware onto their computer by opening an email attachment, clicking on an ad, following a link or even visiting a website that's embedded with malware.

Usually, the attacker requires a ransom payment in cryptocurrency, such as Bitcoin, because it's hard to trace. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever, the ransom increases or the attackers publish the data. When dealing with a particularly unscrupulous attacker, the victim may pay the ransom and still lose the data.

Most ransomware is delivered as a secondary infection after a system is already infected with a Trojan or loader. Many attackers who specialise in these Trojans or loaders then sell access to ransomware organisations. For most organisations, the first line of defense against ransomware is making sure they are protected from other kinds of malware.

What to teach your users

Ransomware is a people-centric threat—so users play a significant role in protecting themselves and their organisations from this cyber attack. Attackers are constantly evolving their tactics, so even technical controls and the efforts of IT security teams can't prevent all malware threats from reaching users.

To help users become successful defenders against ransomware, make these essential dos and don'ts part of your security awareness training on this critical topic.

DON'T click on, download attachments from or reply to suspicious emails.

Look carefully for signs that a message might be suspicious. Ask yourself:

- Is this communication normal—and, if not, was I expecting it?
- Is this message from someone I don't know or haven't communicated with before?
- Does the message contain unexpected content?
- Does the sender attempt to create a sense of urgency or fear? (For example: "Click now or we will lock your account.")
- Does the message ask me to reset my account or enter my credentials?
- Does the sender request that I provide data that's sensitive or not?
- Does the message want me to take some type of action? (For example: "Can you call me?" or "Can you update these details?")

DO understand that not all malicious emails will be overtly suspicious.

Attackers will often use well-known brands or try to make the message appear as if it's coming from someone you know and trust, like your colleague or manager. To avoid missteps, consider:

- Calling or texting your colleague to confirm that they sent the message
- Using a search engine to navigate to the vendor's website to verify the communication or request originated from that vendor

DON'T browse suspicious websites or download suspicious applications.

Here are three tips related to this recommendation to provide to users receiving ransomware security awareness education:

- If a website sounds too good to be true—like offering unlimited free music, movies and apps—it probably is and could even be malicious.
- Know that applications, even those found in popular app stores, can still be malicious. Exercise caution and look for apps from well-known publishers with a high number of downloads.
- Plug-ins for browsers, email or other applications can be just as dangerous as malicious applications. Check with the IT department before downloading and using any plug-ins.

DO report anything suspicious—even if you made a mistake!

It's always best to let the IT or security team know if something went wrong, such as:

- You received a suspicious email that may be a phishing email.
- You received an email that looks like it's from a colleague but seems suspicious or unexpected.
- You accidentally clicked on a link, filled in your credentials or downloaded an attachment and realised it may be malicious.
- You visited a website that seemed legitimate, but afterward sensed something wasn't right.

SECTION 6

Insider Risk

The last few years have wrought a maelstrom of change in the modern workplace. Remote and hybrid work, a widespread embrace of the cloud and increased employee turnover have made safeguarding data more challenging than ever. It's no wonder that insider threats jumped 44% in 2022.[10]

According to the *2022 Voice of the CISO* report, many cybersecurity leaders consider a proactive stance toward insider threats to be essential. After all, no business is immune to insider risk. In fact, insider threats are the top security concern for chief information security officers (CISOs) globally. More than a third of the CISOs surveyed said addressing insider threats is a top priority for their IT department over the next two years.[11]

10 Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.
11 Proofpoint. "2022 Voice of the CISO." May 2022.

What is insider risk?

An insider is a person who has some type of working relationship with an organisation. Because of their role and privileges, they have (or once had) authorised access to critical data and systems. An insider might be a current or former employee, contractor or business partner who might meet all or some of these criteria:

- They have computer or network access supplied by the company.
- They develop products and services for the organisation.
- They know about the organisation's future strategy.
- They have access to protected information.

In short, an insider is someone in a position of trust. Clearly, these users pose a threat when they act with malicious intent and knowingly use their trusted position for personal gain or benefit. What might not be as obvious is that users who accidentally misuse or mishandle their access can cause just as much harm. The same goes for users whose insider access is compromised and exploited by an outside attacker.

The expressions "insider risk" and "insider threat" are sometimes used interchangeably, but they are not the same. Insider threats are a subset of insider risk. All insiders pose risk to an organisation given their access to an organisation's data and systems. But not all insiders become an insider threat. This is an important distinction that requires a strategic and tactical approach to manage effectively.

Types of insider threats

Here's a closer look at the three key types of insider threats:

Careless

A careless insider is a well-intentioned user who makes poor decisions that can result in the exposure or theft of valuable data. Examples include downloading files to a USB storage device or inadvertently sharing sensitive data externally (such as a customer's credit card information). Careless users account for 56% of insider incidents.[12]

Threats from careless user stem from:

Human error. This can include anything from server misconfigurations to sharing a file more widely than necessary.

Bad judgment. This can include taking shortcuts that unintentionally put the organisation at risk, such as moving a file to a USB drive or personal file-storage account.

12 Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

Malicious

These insiders are motivated by personal gain and seek to harm to the organisation. Examples include exfiltrating financial data or trade secrets or destroying sensitive information. Ponemon's research on insider threats found that malicious insiders account for more than a quarter (26%) of all insider incidents.[13]

Threats stemming from malicious users might include:

Sabotage: The malicious insider seeks to damage company systems or destroy data.

Fraud: The insider with malicious intent steals or alters data to create deception with an aim to disrupt the company or benefit financially.

Intellectual property (IP) theft: Any proprietary information that is valuable to an organisation can be considered IP. Malicious insiders steal IP for their own financial gain or to cause long-term damage to the company, monetary or otherwise.

Espionage: When a malicious insider steals sensitive trade secrets, files and data from an organisation and then sells that information to the company's competitors or even state-sponsored threat actors, they are engaging in espionage.

Compromised

Compromised users are often Very Attacked People™ (VAPs) with privileged access to information. In other words, they have credentials and access that could give threat actors access to a company's critical systems and data. Attackers use social engineering techniques such as phishing to steal those credentials. About 18% of insider incidents this year have involved stolen credentials.[14]

Insider threats from compromised users typically stem from one or more of the following:

Stolen credentials

Phishing

Malware

Unintentional aiding and abetting through social engineering attacks

13 Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.
14 Ibid.

What to teach your users

Organisations should help employees avoid being part of the insider threat problem. This learning process starts with building their knowledge about careless behaviour and the potential for malicious insider activity. And while security awareness won't stop users with malicious intent, it can help others recognise and report suspicious behaviour.

Here are key things your users should know about this critical topic:

Think before you act. While taking the shortest path can sometimes make your job—or your colleagues' jobs—easier, it can also create risk. (For example: Don't share account credentials or transfer data to a USB device.)

Stay up to date. Ensure you are aware of the organisation's policies for data and system access and use. (For example: Use only apps and tools provided or sanctioned by the organisation's IT department.)

Report any suspicious behaviour to the security team. If you see behaviour by a colleague that doesn't seem right—for example, the person asks to "borrow" credentials to access an app they aren't authorised to use—they could be a malicious or compromised user.

Also, underscore to your users that they have a critical responsibility to help protect your organisation's data. Encourage them to embrace their frontline role. Incorporating the simple measures outlined above into their everyday practices can go a long way toward reducing and mitigating insider threats.

SECTION 7

Conclusion and Recommendations

People are the new perimeter—anyone can be a target, and anyone can undermine their organisation's security posture with one slip-up or malicious act. Most security leaders understand this reality. But what they really want to know is how to flip the script and turn their organisation's biggest attack surface into a critical layer of defense.

The short answer is that you need to drive behaviour change by building a systemic and sustainable security culture that's customised to your organisation.

But even small changes can lead to big improvements—especially when it comes to strengthening cybersecurity in your organisation. But to build security awareness among your users and motivate them to be active defenders against cyber threats, you need to change your environment.

Moving the needle on change won't happen overnight. But subtle behaviour changes that turn into tiny habits over time can make a tremendous impact.

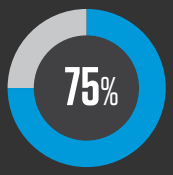
For more security awareness information and resources, visit the Proofpoint Cybersecurity Awareness Hub.

Why Proofpoint

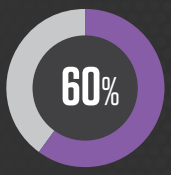
Every day, we analyze more than:

2.6B EMAILS	**49B** URLS	**1.9B** ATTACHMENTS
1.7B MOBILE MESSAGES	**430M** WEB DOMAINS	**143,000** SOCIAL MEDIA ACCOUNTS

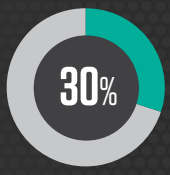
We are trusted by more than:



OF THE FORTUNE 100



OF THE FORTUNE 1000



OF THE FORTUNE GLOBAL 2000

8,000 ENTERPRISES

200,000 SMALL BUSINESSES

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.