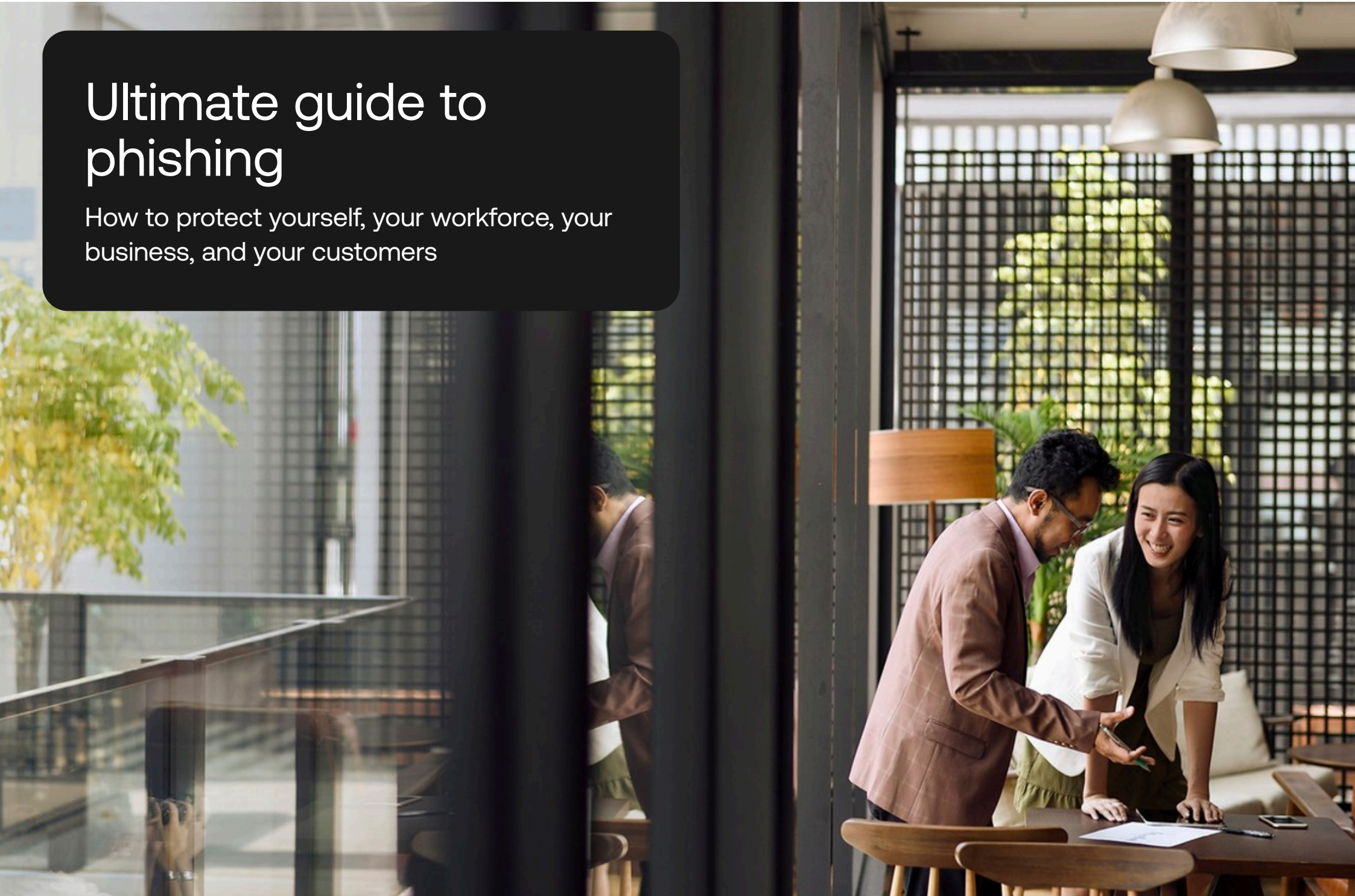
okta
The World's Identity Company

Ultimate guide to phishing

How to protect yourself, your workforce, your business, and your customers



What is phishing

okta

The World's Identity Company

Knowledge is key to fighting phishing

Sixty-eight percent of all data breaches involve the human element, such as human error or a person falling victim to a social engineering attack, according to the Verizon 2024 Data Breach Investigations Report. An attacker doesn't need a zero-day vulnerability to break into your systems. The most powerful tool in their arsenal is simple trickery.

Phishing was the second-most common cause of data breaches. This term describes how an attacker can gain information or access by impersonating a third party: like a colleague, business, government agency, friend, or relative.

The early history of phishing

In 1995, the internet was a place of endless fascination and potential. A screeching 28.8kbps dial-up modem was the latest in high-speed home networking technology, and it connected you to a growing global community. And yes, it was expensive.

Back then, many people paid by the minute to get online. Or they paid for packages that, by today's standards, were eye-wateringly expensive. For those unwilling or unable to pay, they had an option.

An enterprising young hacker called Koceilah Rekouche — someone who, although crossing legal and ethical boundaries, was primarily motivated by a sense of curiosity and exploration, rather than the outright malice of today's organized threat actors — created a tool called AOHell.

It could generate fake credit card numbers for new trial accounts. Or, it could help you steal someone else's legitimate account by sending an email that purported to come from AOL security and asks for their username and password.

The last bit was called a 'fisher' tool. And because at that time hackers would substitute 'f' with 'ph', fishing became "phishing."

That's the first recorded usage of the term that now strikes fear into the hearts of anyone who owns a social media page, has an email account, or runs a business. Phishing is no longer something used by people wanting to get online for free. It's a big business.

The state of phishing today

Researchers identified 500 million phishing attacks in 2022. That figure is double the previous year's. And the impact of a successful phishing attack can prove devastating. Figures from IBM put the average cost at a cool $4.91 million. A business email compromise (BEC) attack — a subtype of phishing where a malicious actor tries to convince a company executive into making large payments or sharing confidential information — can cost $4.89 million.

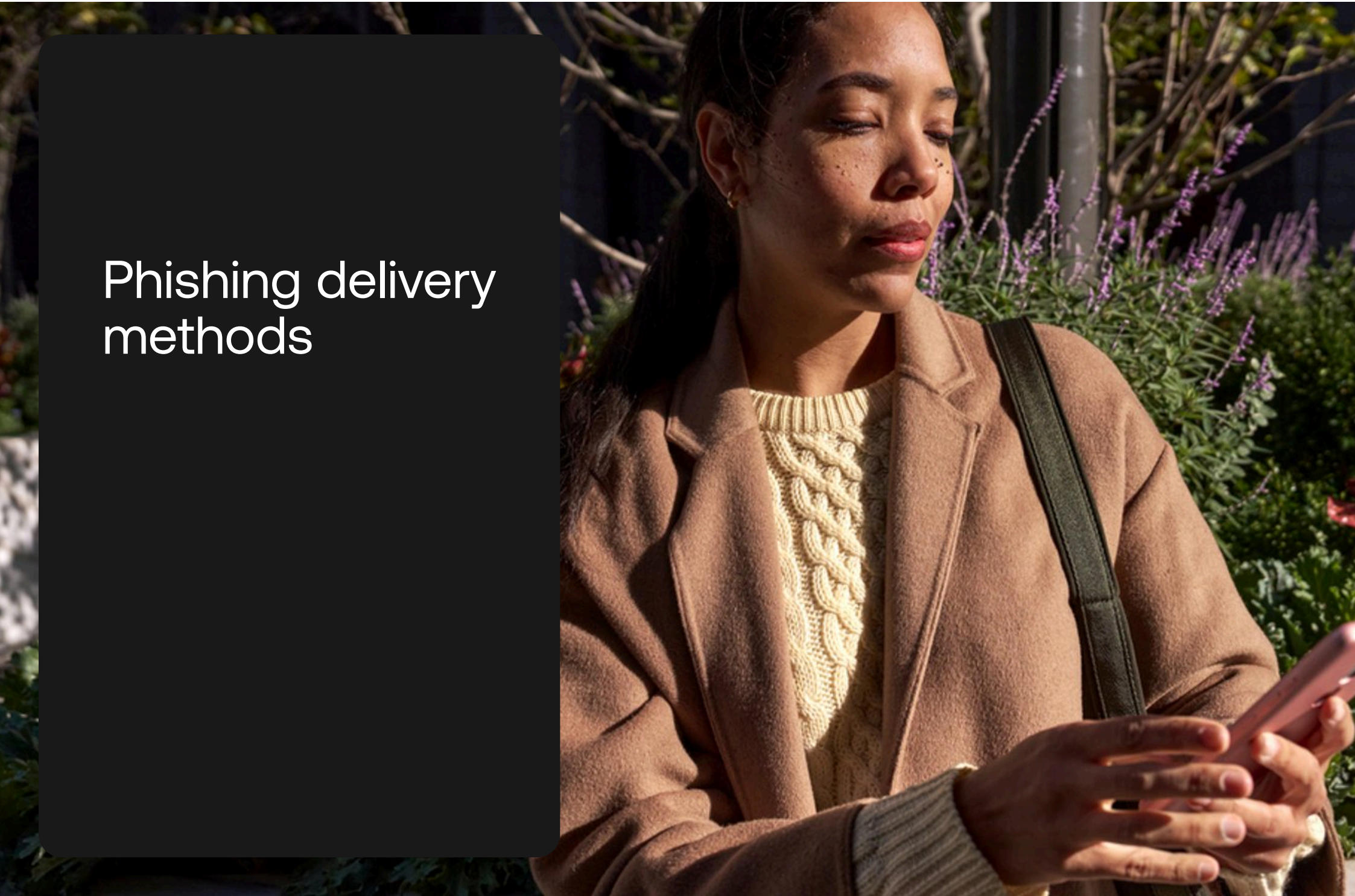
Ultimately, phishing is just another type of deception. Something that's as old as humanity itself. Lies and misdirection have an incredible destructive potential — just ask the Trojans. But what makes phishing such a terrifying prospect is that it can happen at scale. It's both a hammer and a scalpel.

An attacker can send millions of emails in the hope that a handful of recipients take the bait. Or they can

build something that's unique for one person, or one company, in the hope of a massive payday.

Later we'll walk you through the different kinds of phishing and how malicious actors use them. But we'll start with the very near future, where advances in artificial intelligence technology promise to make phishing an even more dangerous threat.

Phishing delivery methods



Phishing types and how they work

Phishing comes in all shapes and sizes. As technology evolves, so too do the strategies and tactics of attackers. A threat actor's methods change to meet their objectives and opportunities.

In this section, we'll explore the various types of phishing attacks and how they work. Let's start with understanding all the ways in which an attacker can send a phishing attack. The overall technology or communication system that is leveraged to deliver the malicious message matters – both in terms of its effectiveness, but also who it reaches.

Email or phishing

The term “email phishing” encompasses a broad range of phishing tactics. These vary, not merely in how they work, but who they target.

For consumers, perhaps the most easily recognizable type is “clone phishing.” This is where an attacker impersonates an existing business in order to extract sensitive information, user account details, or money.

Clone phishing emails are often sent in huge volumes to vast lists of email addresses. While this approach isn’t particularly sophisticated, the emails themselves often are, faithfully replicating the style and language of the brand being impersonated. According to 2022 research from Tessian, the five most commonly impersonated brands in phishing emails are: Microsoft, ADP, Amazon, Adobe Sign, and Zoom.

In the case of high-value targets, an attacker will take a more refined approach. One approach, which we’ll explore later, is “spear phishing,” where an attacker will craft phishing messages intended for small and highly-specific audiences. These audiences can be a single person, or they may include every employee at a given company.

Phone call or vishing

Vishing is a portmanteau of “voice” and “phishing.” This tactic sees an attacker try to social engineer a victim using the phone or another comparable VOIP service, like FaceTime or Skype. The goal is to persuade victims to provide sensitive information, or to perform a specific action, like transfer money or download malware.

An attacker may, for example, choose to masquerade as a representative of a well-known company. Or they may impersonate someone known to the victim. This doesn’t merely increase their credibility with the victim — it also allows them to create a sense of urgency.

In one recent case, an attacker impersonated a Newfoundland man

and convinced his parents to wire almost $10,000 CAD for bail fees following a fictitious road traffic incident. In this case, authorities suspect the attacker used an AI-generated “deepfake” of the son’s voice.

In a separate 2019 case, an attacker convinced the CEO of a UK-based energy firm to transfer €243,000 to a bank account under their control after impersonating the head of its German parent company. Again, authorities believe the attacker used an AI-generated deepfake to accomplish their goals.

Text message or smishing

The term “smishing” is a portmanteau of “SMS” and “phishing.” But don’t be fooled. Smishing can occur on other non-SMS messaging platforms like iMessage, WhatsApp, Viber, and others.

As with the other tactics we mentioned, the goal of a smishing campaign is to trick the recipient into sharing information they otherwise wouldn’t, or to perform any other secondary action, like share their credit card or banking details, or download a piece of malware.

Smishing affects both individual consumers and businesses alike. As with email-based phishing, there are examples of large-scale “spray-and-pray” smishing campaigns, and those intended for smaller audiences.

As Kaspersky notes, smishing can prove highly effective because, while many people are aware of the risk of email-based scams, they may mistakenly believe that SMS and messaging apps are comparatively safe and let their guard down.

Additionally, because text messages are simpler than emails, the attacker doesn’t need to work as hard to mimic the style and appearance of an established brand.

As with email phishing, smishing campaigns can be automated, with messages sent at an incredible velocity. In 2021, UK police arrested an individual responsible for a phishing campaign that sent 26,000

SMS texts in a single day. The messages purported to be from Hermes (now Evri), a European parcel delivery company, and attempted to solicit bank details from the recipients.

Social media phishing

According to the Pew Research Center, around 70% of Americans use social media to connect with friends, relatives, and businesses. This makes it an enticing target for threat actors, who seek to exploit a person's connections for their own purposes.

As the LA Times notes, a common tactic on professional networking site LinkedIn sees attackers publish fake job advertisements. Candidates who respond are then bombarded with an escalating series of requests for personal and financial information.

On platforms that are centered around person-to-person interactions, particularly Facebook, an attacker may create a replica of an individual's profile and send friend or message requests to their contacts. Under this assumed identity, they will often direct the recipient to external sites, where the attacker will attempt to obtain their login credentials or credit card information.

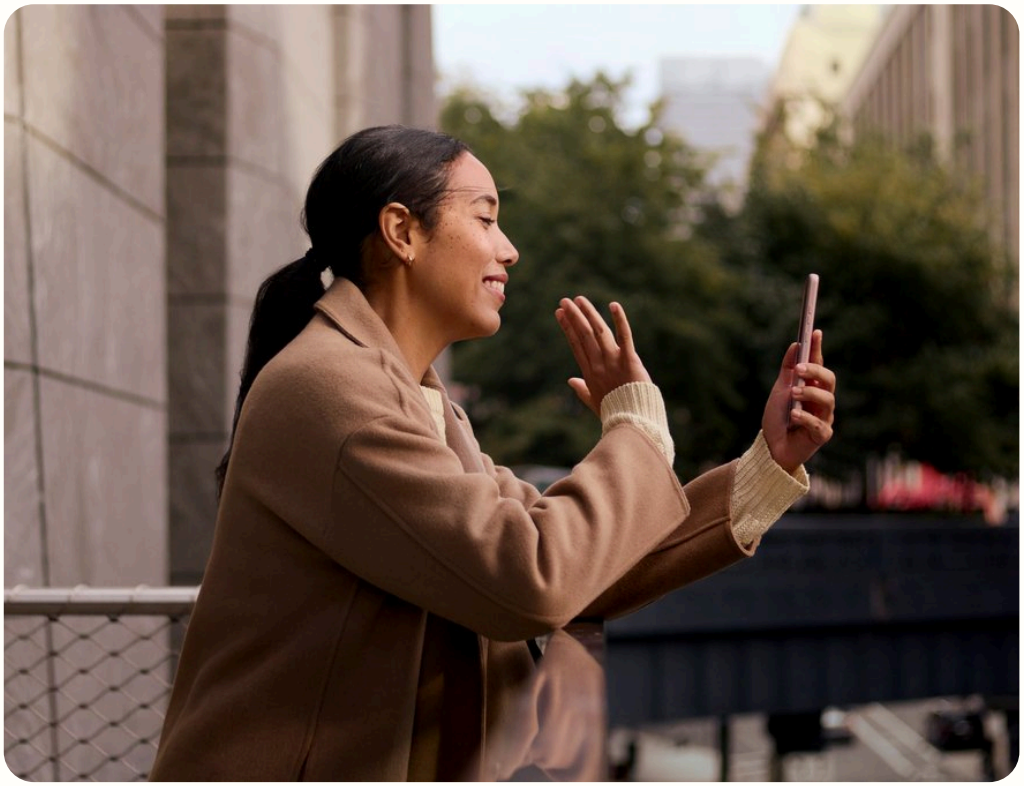
Another approach used by attackers exploits our innate senses of curiosity and shame. Impersonating a trusted individual, the attacker will send messages that ask: "Is this you?" The message will include a link with a thumbnail that, although small and blurry, obviously depicts an explicit or salacious act.

The recipient, after clicking the link, is taken to a webpage that accurately mimics the homepage of a given social network. If they attempt to log-in, the attacker will obtain their username and password.

Social media phishing takes many forms. It would be impossible to exhaustively list them here. While platforms strive to protect their users, blocking the accounts of malicious users as soon as they're detected, the best defense is a constant state of vigilance.

QR code phishing

QR codes are a type of barcode used to encode information, like website links, contact information, or text. They provide a convenient way of accessing information or



websites without the need to type anything.

But they can be abused in phishing scams. In 2022, the FBI warned consumers to be wary when scanning QR codes following a series of high-profile security incidents. The Bureau highlighted incidents of fake codes on physical restaurant menus and within emails that, when scanned, led to malicious websites.

Across several cities in Texas, including Houston and Austin, scammers placed QR code stickers on parking meters. The codes, when scanned, directed the victim to a website under their control that captured their payment information. It's not known how many fell victim before the stickers were removed.

Since QR codes don't include any visible text, it's impossible to identify whether they link to a legitimate or malicious website. Email security technologies are often unable to check the images to identify potentially harmful links. The only way for an individual to know for certain is by scanning the code with their device – which, obviously, presents an element of risk.

The only real safeguard is to exercise extreme vigilance, both when choosing what codes to scan, and when the page eventually loads on their phone.

WiFi or "evil twin" phishing

An "evil twin" attack takes advantage of a person's trusting nature when connecting to a public Wi-Fi hotspot. The attacker creates a fake hotspot that, while appearing to be legitimate, is designed to harm the user by monitoring their traffic and redirecting them to websites under the attacker's control.

The attacker could, for example, create a fake sign-in portal designed to capture a person's private information or credentials. Or they could intercept requests for legitimate websites and send the victim to a facsimile that, although appearing genuine, is actually a fake designed to steal their information or login details.

Phishing tactics

Inside malicious actors’ tactics

Malicious actors have multiple ways to deliver a malicious message whether it is through an email, a phone call, or even Wi-Fi. But depending on their motivations and targets, they will follow different tactics when leveraging these technologies.

Untargeted phishing

While the tactics described above often involve a direct person-to-person interaction between the attacker and the victim, a significant percentage of phishing attacks are fundamentally undirected. The attacker doesn't have a target in mind, but simply chooses to send a large volume of malicious texts, emails, or phone calls in the hope that a small percentage takes the bait.

While undirected phishing attacks lack precision, they're easy to operate at scale. The attacker simply needs a list of targets — often obtained from previous data breaches — and the technology to bulk-distribute their malicious messages.

Angler phishing

Angler phishing attacks typically — but not always — occur on social networking pages and see an attacker impersonate a customer service representative in order to extract information or money from a victim.

Unlike other types of phishing, the attacker doesn't need to know anything about their victim. Whereas smishing/vishing and email phishing require valid phone numbers and email addresses, someone perpetrating an angler phishing attack only needs to search for a complaint about a business, or a request for support.

The attacker will then direct the victim to a private channel, where they will then use social engineering tactics to extract information from the victim, or try to trick them into performing an action.

The businesses impersonated vary, but banks and credit card companies are more likely to be spoofed. According to one study from ProofPoint, over half (55%) of angler phishing attacks involve financial institutions.

Business email compromise

A business email compromise (BEC) attack describes a broad array of methods used to trick a high-ranking company executive or official into performing an action, transferring funds to an account under the attacker's control, or revealing potentially sensitive information.

There are many manifestations of BEC attacks. A malicious actor could, for example, create a superficially legitimate email address to pose as a company CEO (or, having previously compromised their email account, use their actual email address) and request that an employee makes a transfer to an offshore bank account.

Alternatively, they could pose as a foreign supplier and issue a bogus invoice, hoping that the company pays it before they properly scrutinize it. While the methods and motivations may vary, they all rely on email to work, and often involve senior company personnel, who are either the targets of an attack or the subject being impersonated by an attacker.

It's no surprise that the FBI describes BEC phishing — also known as email account compromise (EAC) — as "one of the most financially damaging online crimes." According to the Bureau, losses from BEC scams reached $2.4 billion in 2021, up from $300 million in 2016.

AitM phishing

AitM (adversary-in-the-middle, sometimes referred to as "man-in-the-middle" or "meddler-in-the-middle") phishing sees an attacker intercept a victim's network traffic with the aim of altering the appearance of websites, or redirecting the victim to a website under their control. This often involves a sophisticated piece of malware being deployed on the victim's computer.

One common approach, as noted by Palo Alto Networks, sees the victim presented with a facsimile of a login page. This facsimile is the "adversary" or "meddler." It captures the person's login details and relays them to a computer under their control.

If the site uses MFA (multi-factor authentication), the spoofed webpage will continue impersonating the targeted website and ask the user for a one-time passcode. When the user successfully logs in, the AitM server receives a real session cookie, allowing the attacker to access the victim's account. The server may also continue to act as a proxy, allowing the victim to use the website, albeit with their traffic relayed through the attacker's computer.

This approach is particularly pernicious, not merely because it can bypass many of today's MFA systems, but also because it's completely invisible to the victim. Whereas email phishing attempts often include some discrepancies that can arouse suspicion, like clunky syntax or visual discrepancies, this approach has no tell-tale signs. Nothing to indicate that anything is amiss.

Spear phishing

The term "spear phishing" broadly describes a type of targeted phishing attack. Its victims can include private individuals, employees of a specific organization or business, or even its senior leadership.

The goal of a spear phishing attack is to obtain information that will be useful for the attacker — such as account credentials, proprietary company information, or access to the company's system — or to induce the target into performing a specific action. This might include

transferring funds, clicking a compromised link, or opening a malicious email attachment.

Because spear phishing attacks are customized for each victim or target organization, they're often harder to detect through technological means. Whereas a spam filter can identify phishing emails sent to millions of addresses, they may struggle to identify a phishing email intended for an audience of one.

Email is a common channel for spear phishing attacks, but it isn't the only one. Attackers will use any channel that helps them accomplish their goals, including SMS, instant messaging, and even phone calls.

The targets of phishing attacks

okta

The World's Identity Company

Tantalizing targets come in all sizes

Just like phishing methods vary, so too do the potential targets.

Businesses of all sizes, from the largest S&P titan to the smallest “mom-and-pop” shop, are at risk. Phishing attacks can impact senior business leaders and high-net-worth individuals, but they can also harm ordinary people too. And that’s because no matter who you are, your job, or your financial status, your data has value.

Ultimately, people who participate in phishing attacks are opportunists. They go after whatever will bring them the biggest returns. And so, some targets are more tantalizing than others.

Cryptocurrency tools, wallets, and platforms

In the period between January 2021 and March 2022, Americans lost over $1 billion to cryptocurrency-related fraud according to official FTC statistics. Business and government impersonation scams accounted for $133 million of these losses. Romance scams were responsible for a further $185 million.

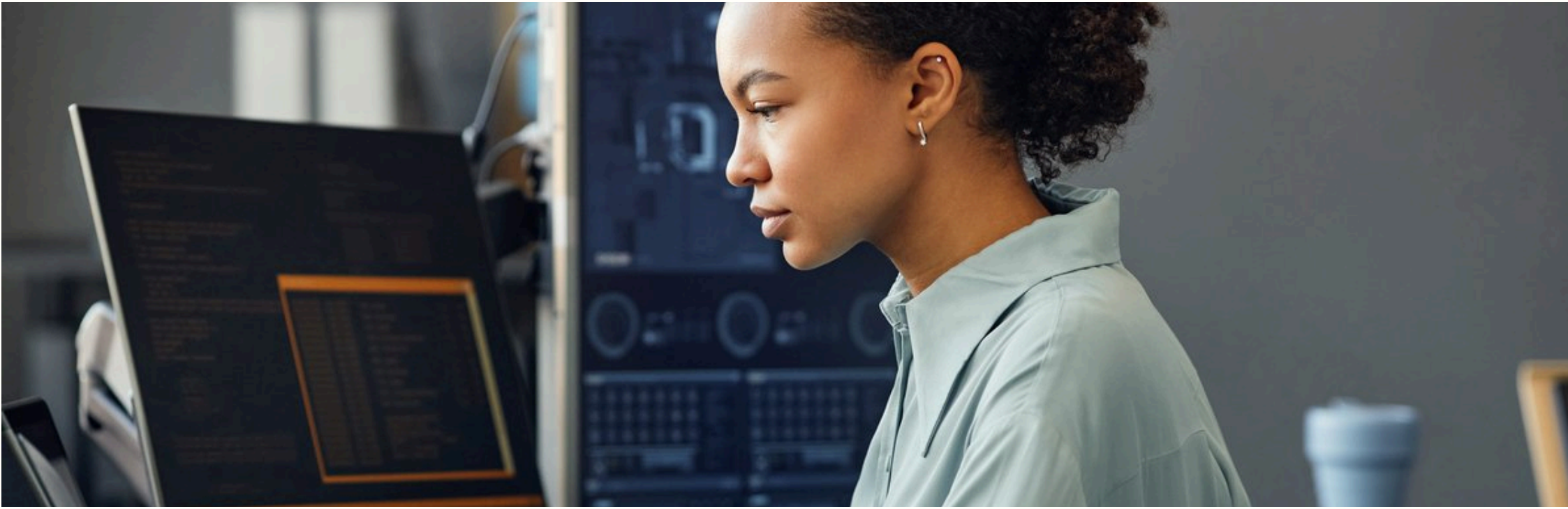
Reliable data is hard to find, but the use of phishing in cryptocurrency scams is a well-documented phenomenon. And it's easy to understand why.

For a malicious actor, cryptocurrencies offer several major advantages. Transactions are, by their very nature, irrevocable. Unlike credit card transactions, there's no chargeback mechanism for Bitcoin.

And, since cryptocurrencies are largely decentralized and deregulated, an attacker can easily transfer their funds across borders and jurisdictions. Although the blockchain allows an external observer to track the flow of transactions, malicious actors have tools and tactics to obfuscate the direction of funds, from tumblers to "privacy coins" like ZCash and Monero.

VIPs or "whaling"

Whaling is a subset of spear phishing. What sets it apart is the



fact that its targets are high-value individuals, or senior figures within an organization.

For an attacker, a "whale" is a highly lucrative target, and so they'll spend time crafting a phishing email that's most likely to resonate. Whaling emails are even more customized than a standard spear phishing email.

According to the UK's National Cyber Security Centre (NCSC), they'll include "personalized information about the targeted organization or individual," convey a sense of urgency, and use the language and tone of a business email.

As with other phishing emails, the goal is to induce the victim into performing a secondary action. These could include providing sensitive information, installing a piece of malware, or transferring funds.

In a growing number of cases, the attacker will phone the victim after sending the whaling email. According to the NCSC, these calls are used to confirm receipt of the email, and to reinforce the credibility of the message.

Catphishing

The term "catphishing" is a portmanteau of "catfish" and phishing. Catfish is a slang term for someone who engages in a romantic relationship with another online while also misrepresenting their identity.

Catphishing scams occur primarily on social networking and dating websites. An attacker will create a fake profile with the aim of luring a victim into a fake relationship with the goal of exploiting them for money or personal data.

The motivations behind a catphishing scam vary. As Panda Security notes, an attacker may wish to financially exploit their victim, obtain personal information that could prove useful in other crimes, like fraud or identity theft, or simply seek to obtain their photos and personal information in order to conduct further catphishing attacks. Catphishing falls into the broader category of romance scams, which cost US victims at least $1.3 billion in 2022 alone, according to the US Federal Trade Commission. Law enforcement agencies received almost 70,000 reports of romance scam crimes, with the median reported loss being $4,400.

Tax season

Although tax season can inspire feelings of dread among workers and businesses alike, it can prove a highly lucrative time for online fraudsters.

During the 2023 tax season, the IRS warned tax professionals and businesses to be wary of spear phishing attempts, particularly those centered on Form W-2. This document, produced yearly for each employee, provides the IRS with a breakdown of taxes withheld and wages paid by the employer. Identity thieves can use these to file fraudulent tax returns on behalf of the employee and obtain refunds.

It also urged consumers to remain vigilant of emails and texts purporting to come from the IRS, particularly those that mention a tax refund or a potential tax issue.

These phishing attempts — which IRS Commissioner Darry Werfel described as “relentless” — are almost always fraudulent, with the agency choosing to communicate with individuals via postal mail.

Workplaces

Some of the most impersonated brands in phishing emails are workplace tools: like Microsoft (and particularly Microsoft Office 365), Zoom, and ADP. These applications inevitably contain sensitive information, from proprietary business records and intellectual property, to payroll information and tax documents.

Job roles, teams, and industries

Phishing threatens everyone, but some industries and job roles are more likely to be targets than others. According to 2022 data from Egress, finance and IT teams are the most likely company departments to be targeted by phishing emails.

Data from Q1 2022 shows the healthcare sector as the most common target of phishing attacks. Technology businesses were close behind, with the software-as-a-service (SaaS) , e-commerce, social media, and cryptocurrency sectors accounting for the rest of the top-five targets.

Even if your organization doesn’t operate in these sectors, you should still be vigilant. Research from Egress shows that 84% of organizations were victims of phishing in 2022. Whoever you are, your data and your relationships have value to an attacker.

Individuals

Public sector organizations and corporations are frequently the target of phishing attacks, purely because — on a financial basis — they’re often the most rewarding. But individuals shouldn’t let their guard down.

While you might not be a large NASDAQ or S&P business, your information holds value to a malicious actor.

An attacker may wish to gain access to your online streaming TV subscriptions — like Netflix or Hulu — to resell them for a profit. Your email and social media accounts could be used to conduct further phishing attacks against your friends, family, colleagues, and employer. And, with access to your financial applications, an attacker can steal your funds or submit fraudulent tax returns on your behalf.

And so, it's important you never let your guard down — both at work, and in your private life.

Jobseekers

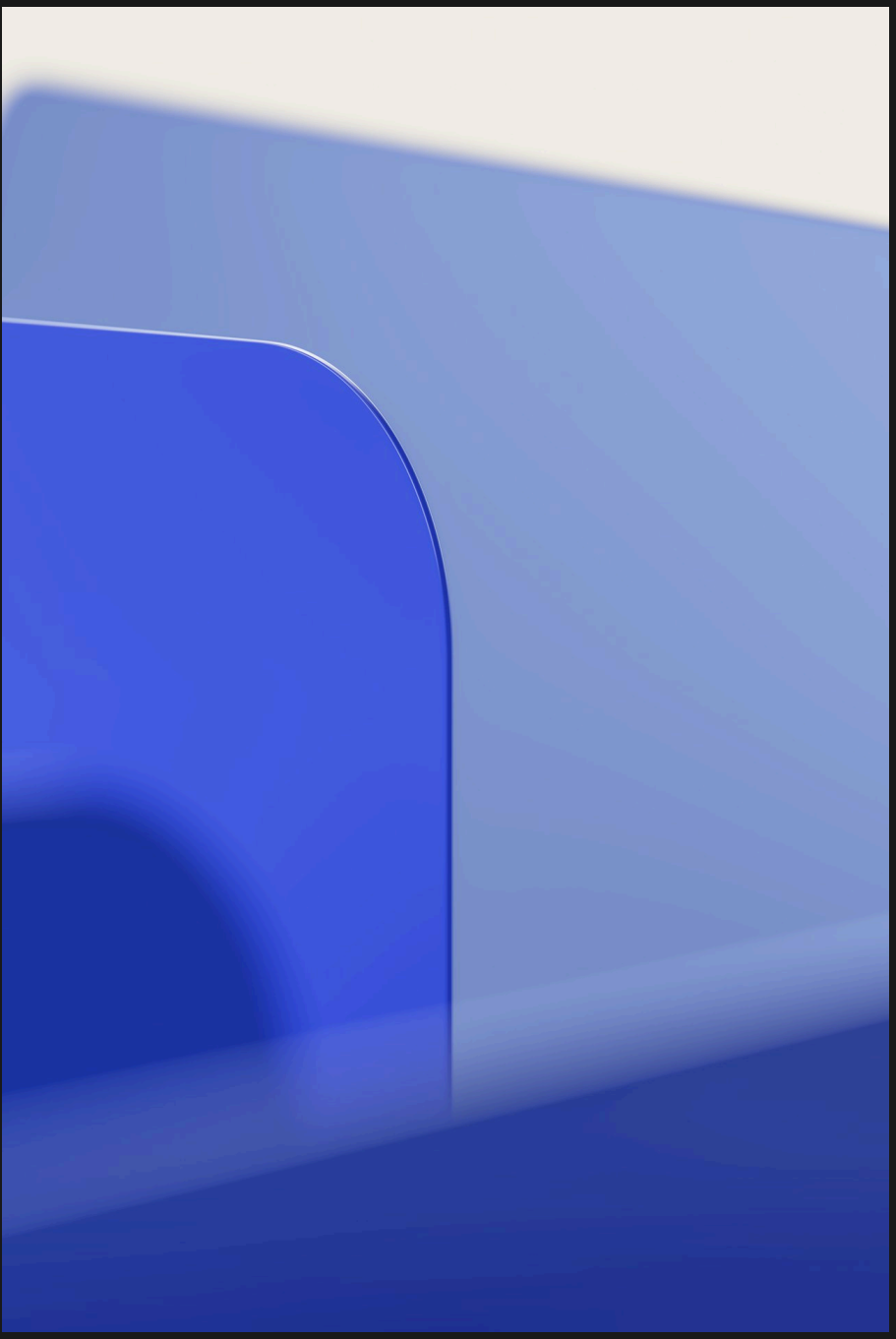
Recruitment scams are an increasingly common tactic that exploits a person's desperation to find a job.

Here, an attacker impersonates a recruitment agent or HR worker and, using email or a business social networking site like LinkedIn,

reaches out to someone looking for a new role. The candidate will likely provide their resume. This can be used for further phishing attempts, or as a means to plant an "insider" at an organization, as documented with certain state-sponsored actors.

The attacker may also try to use the promise of employment as a means to extract money from the victim, or to induce them into performing actions that are otherwise harmful or malicious. In one example reported by Sky News, a victim was told to pay out-of-pocket for a training course and a "burner" phone. His job then saw the victim try to recruit others into the same scheme.

Procedures



Scam mechanics revealed

We've talked about the tactics used by phishing scammers, as well as the methods they often employ. But we're yet to dive into the actual mechanics of a scam.

When it comes to gaining trust, operating at scale, and transferring money, phishing scammers have a number of tools at their disposal. Some are relatively old, while others are on the bleeding-edge of technology.

Cryptocurrency payments

Digital currencies are designed with decentralization in mind. This, inevitably, means there are fewer protections than you'd find in the traditional financial system, like the ability to block or reverse a payment, or to claw back funds stolen from your account.

It's for this reason that phishing scammers often target cryptocurrency users and services. But they often use cryptocurrencies to transfer funds across borders, and to obfuscate the identities of those receiving the proceeds.

An attacker may use something called a cryptocurrency tumbler to cover their tracks. These systems pool, mix, and shuffle funds in a way that makes it almost impossible to identify the origins of funds. In essence, they mix "clean" cash with "dirty" cash in a way that prevents an observer from determining which is which.

According to a 2022 report from Chainalysis, "illicit" cryptocurrency addresses were responsible for 23% of all mixer transactions that year. Many of these addresses belong to known criminal actors that use phishing tactics as a routine part of their business.

An example is the Lazarus Group, which the US State Department believes to be controlled by the North Korean government, and has used phishing extensively when targeting individual cryptocurrency owners, as well as businesses in the cryptocurrency sector.

Generative AI

The term ‘Generative AI' describes a type of artificial intelligence where computers produce bespoke creative works that, until recently, could have only been created by a human. Harnessing the powers of deep learning and large language models (LLMs), as well as large datasets and powerful training hardware, these AI models can create complex written, video, and visual works in a matter of seconds.

Generative AI has the potential to revolutionize countless industries, improving productivity and quality. But in the wrong hands, it can be a tool for harm.

Malicious actors could, for example, use a generative AI system to produce customized phishing emails at an incredible scale or velocity, increasing the probability of being successful. Text-based generative AI systems aren’t just fast. They’re also designed to write like a human. Unless told otherwise, they use standard spelling and grammar. And so, they have the potential to be more convincing than a traditional human-generated phishing email, even to the most cautious person.

An attacker could even synthesize the voice of a CEO and use it to trick employees into sharing proprietary company information with a third-party. The VALL-E model can create a replica of a person’s voice from a three-second recording. If the attacker can provide more audio training data (particularly high-quality training data), the quality of the facsimile improves drastically.

As with any technology, generative AI systems can be misused. And so, the companies building them are implementing safeguards.

These protections often restrict the kinds of questions that can be asked. If a generative AI system, like OpenAI’s ChatGPT, detects that a person is trying to craft a malicious email, it’ll refuse the request.

These safeguards are helpful, but they aren’t perfect. There are LLMs

- **Text:** Generative AI models like OpenAI’s GPT-4 and Alphabet’s LaMDA can respond to written requests and produce blogs, explainers, and even poems.
- **Code:** Similarly, some models, including GPT-4 have proven themselves capable of writing software.
- **Audio:** Generative AI can be used to synthesize speech, and models like VALL-E can even create sound recordings designed to mimic a specific human speaker, from their accent to their intonation. Despite still struggling with the “uncanny valley” where something just feels “off” deep fake audio can still fool some listeners, reports the New Scientist.
- **Images:** Models like DALL-E 2 can generate photorealistic images based on a single written prompt.
- **Video:** Some generative AI models, such as Meta’s Make-A-Video system, can produce GIF-like moving pictures from a simple written prompt. Others, including Runway’s Gen-1, have the ability to generate videos from sample images or written text.

that can be run locally with safeguards removed. Over the past few months, we've seen numerous examples of generative AI-driven phishing campaigns. Security researchers have exposed ways in which a generative AI chatbot can be tricked into writing potentially-harmful content.

Phishing has always been a problem for consumers, governments, and businesses alike. Generative AI didn't create this problem, but it has the potential to exacerbate it.

Everyone — employees and private individuals alike — needs to be increasingly vigilant going forward. Even the most sophisticated phishing attack can be defeated by a skeptical and cool-headed mind.

Data breach lists

Since its inception, the website Have I Been Pwned has tracked breaches across 678 websites, totaling over 12.5 billion accounts. These leaked credentials often provide an attacker the information and credentials they need to conduct further phishing attacks.

If a website fails to properly protect a person's password by salting and hashing, an attacker could simply use the victims credentials to impersonate them. But even without that information, leaked data can be useful for an attacker.

By looking at a data breach, an attacker can identify where a person has accounts, and then deliver phishing emails that are both targeted and personalized. This threat isn't hypothetical. After a rogue insider leaked the customer database of the Desjardins Group — a large Canadian financial services organization — the number of phishing URLs associated with that particular brand jumped by 1,680.4%, according to Vade Secure.

The business structure

It's a common misconception that threat actors are universally organized in a way akin to a shadowy underground enterprise, with none of the formalities that are inherent within a legitimate business. The image of a group, working from a murky room illuminated only by the glare of

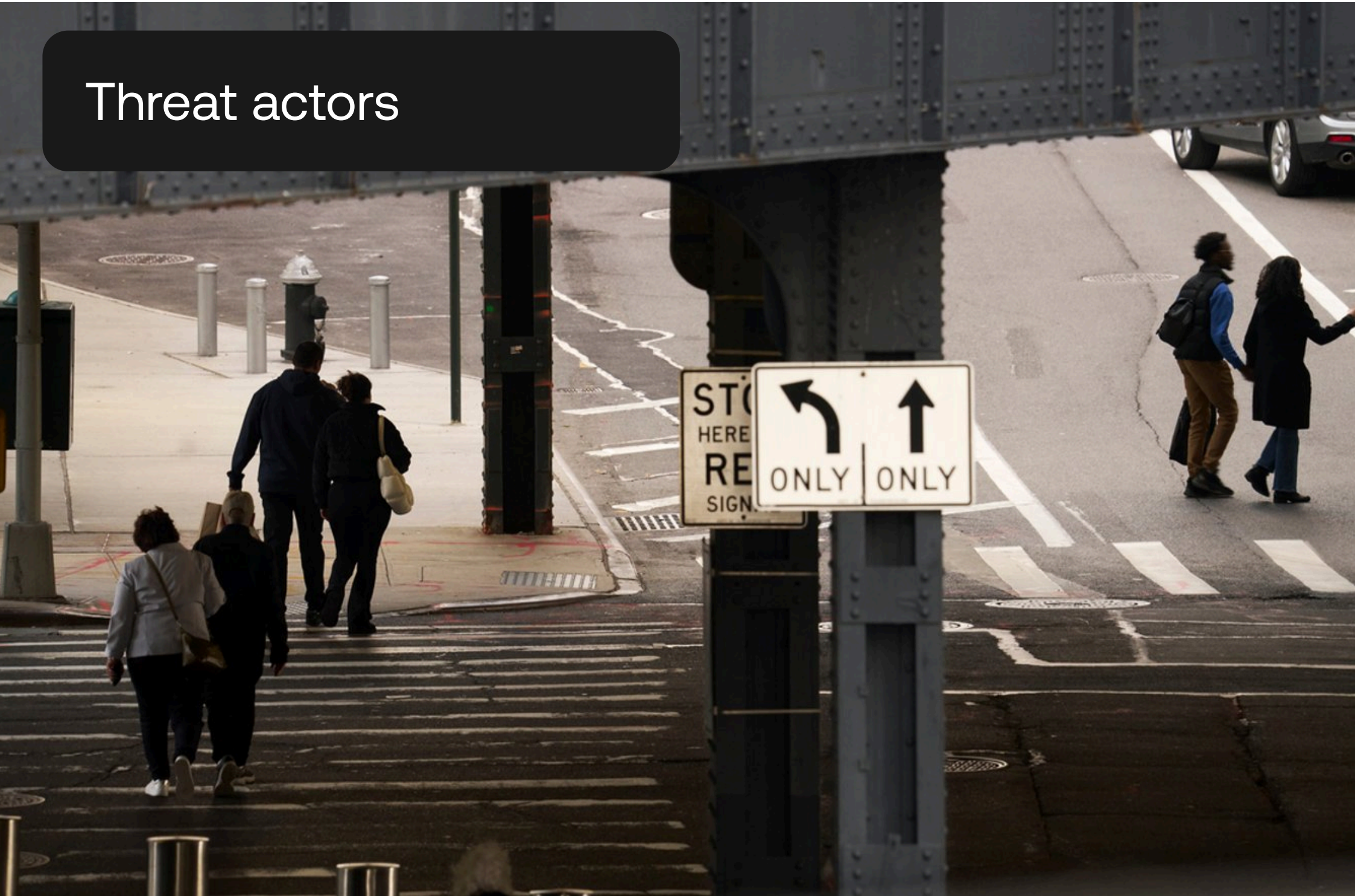
laptop screens, feels natural and obvious.

Reality is a lot more complex. Criminal organizations — including many phishing threat actors — are increasingly well organized. Despite their criminal intentions, they often try to cloak themselves in the veneer of a legitimate business. They'll sometimes rent office space, have payroll and HR systems, and recruit from the wider public, rather than from the denizens of shadowy Dark Web forums.

This trend — as observed by the New York Times, as well as diligent citizen journalists like Jim Browning — is often true for call center scams. These often fall into the category of phishing (specifically "vishing") or are, at the very least, phishing adjacent.

Although portraying themselves as legitimate businesses does expose the organization — and its leadership — to greater external scrutiny, it does have some major advantages. For phishing attacks that are only effective at scale, it gives the threat actors a greater recruitment pool to work from, allowing them to rapidly expand their operations — or simply sustain them in the face of worker attrition.

Threat actors



A dubious distinction: high-profile malicious actors

Phishing can be a highly profitable enterprise. The number of malicious groups and individuals that use phishing tactics is unknowable — although it wouldn't be unreasonable to assume the number measures in the thousands, and perhaps higher.

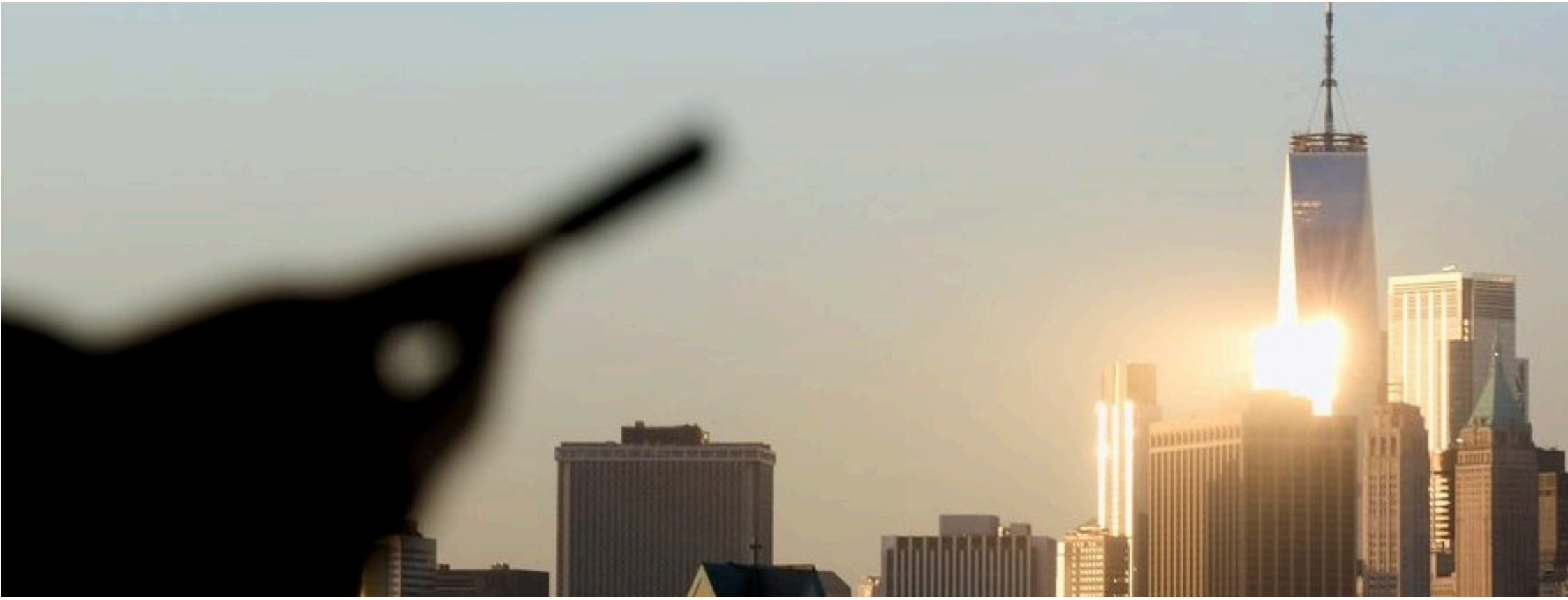
Despite the prevalence of phishing, certain malicious actors have achieved a degree of notoriety (and perhaps even infamy) for the innovative and effective methods they use. Here are three of the most high-profile examples.

The Lazarus Group

North Korea is often described as “the hermit kingdom,” where a combination of crushing international sanctions and an internal policy of isolationism has virtually cut the country off from the outside world. And yet, North Korea is highly reliant on external trade in order to fund the lifestyle of its hereditary leader, Kim Jong-Un, as well as its nuclear weapons program.

To obtain the funds it needs, the country has turned to cybercrime. The Lazarus Group is widely suspected to be the cyberwarfare wing of the North Korean government, and over the past decade, has performed devastating attacks against foreign financial services entities, cryptocurrency companies, and overseas adversaries of the regime.

The Lazarus Group is suspected to be the culprit of the 2017 Wannacry ransomware attack. It has used phishing to spread compromised documents to organizations in the



defense and cryptocurrency space, allowing the group to steal funds and information that could prove useful to North Korea's military.

Its ability to use phishing — combined with the group's sophisticated software engineering skills — allowed The Lazarus Group to steal an estimated $400 million in cryptocurrency in 2021 alone, with both private individuals and startups in their crosshairs.

Fancy Bear

Also known as APT28, Fancy Bear is a state-sponsored cyber espionage group believed to be part of Russia's GRU — its military intelligence organization. As with the Lazarus Group, Fancy Bear relies heavily on phishing methods.

Its targets are predominantly those opposed to the Kremlin, including journalists, supranational organizations (like the World Anti-Doping Agency), and foreign governments and militaries.

Guccifer 2.0

Unlike the original Guccifer — a Romanian man believed responsible for compromising the email accounts of several high-profile US political operatives — Guccifer 2.0 is believed to be a state-sponsored entity under the control of the Russian GRU.

Guccifer 2.0 is most notable for its activities during the 2016 election, where it obtained access to the emails of the Democratic National Committee (DNC) and subsequently leaked the contents to Wikileaks. One of the victims included John Podesta, the chairman of Hilary Clinton's presidential campaign.

To conduct this attack, Guccifer 2.0 relied on phishing emails that impersonated Gmail and warned that the victim's account credentials had been compromised and needed to be reset. Although this attracted the suspicion of many victims, including Podesta, they were nonetheless successful. This was, in part, due to a mistake by a campaign tech employee who described them as "legitimate" when they meant to type "illegitimate."

How to detect and prevent phishing attacks

okta

The World's Identity Company

7 signs of a phishing attack

Threat actors constantly adjust their methods and tactics, but there are still some easily identifiable clues that can help you recognize a phishing attack.

- **A sense of urgency:** An attacker will often pressure their victim into providing information, performing an action, or paying for something. They may tell you your account has been suspended, or that you have an unpaid invoice, and you must take action now. They may use language that suggests you need to act immediately — or else.
- **The email address or domain:** Email phishing attacks sometimes come from public mail providers, or from domains that are crafted to impersonate the company being spoofed.
- **Web links:** Similarly, phishing emails often include web links that purport to come from a legitimate company, but almost always redirect the target to another location. While these websites may look like the real deal, the URL will be for another website.
- **Generic language:** In the case of bulk-sent phishing emails, they'll use a generic greeting like "Dear Sir/Madam," or just "hello."
- **An element of surprise:** If you can't think of a reason why your social media account has been suspended or your bank is trying to get you to verify your information, or you've received an invoice you weren't expecting, it's worth taking a moment to check whether it's legitimate.
- **Attachments:** Be wary of downloading any attachments from senders you don't know or which have not been scanned for viruses by your email provider.
- **Language style:** People have their own unique ways of communicating. If you receive a message from a friend or a colleague but it doesn't sound like them, be cautious.

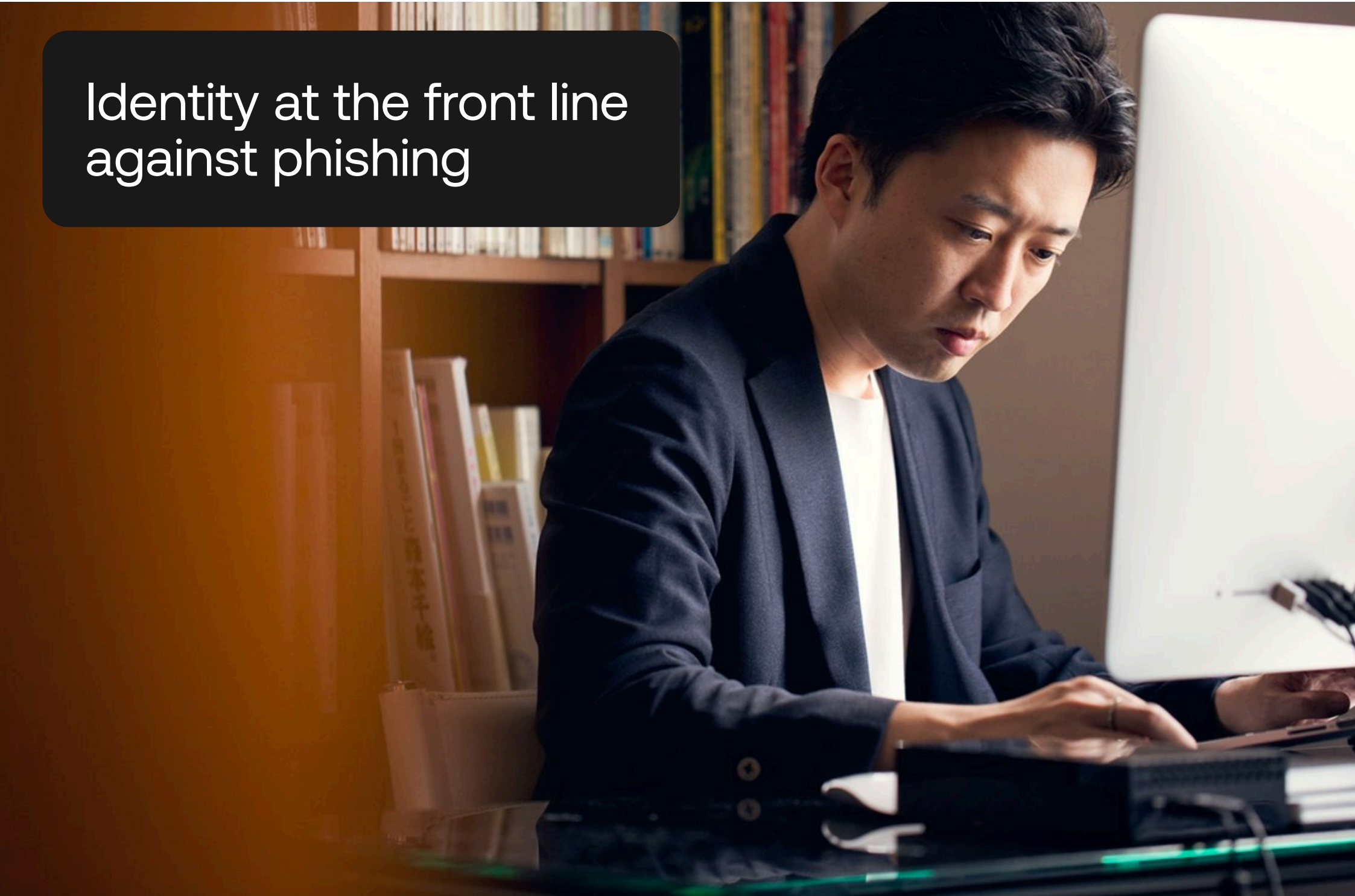
7 strategies for preventing a phishing attack

Phishing can be hugely damaging for individuals and businesses. But with the right tactics, technologies, and training, you can prevent a phishing attack. Here are some tried-and-tested strategies that work:

- Phishing awareness training will teach your employees what to look for, and what to do if they suspect a phishing attack is underway. According to research from Proofpoint published in 2022, 80% of organizations said that phishing awareness training reduced the employee's susceptibility to phishing attacks.
- Reinforce the awareness training with a simulated phishing attack. These show employees what a phishing attempt would look like in the real world, and how to apply the theory they've learned. According to research from the Infosec Institute, phishing simulations can double learning retention within 12 months. This means your employees are more vigilant against phishing attacks for longer.
- Use MFA in your professional and personal lives. This isn't a silver bullet, but it can drastically reduce the risk of a successful account takeover from a phishing attack.
- Deploy an endpoint protection tool. These often include anti-phishing features, including a blacklist of known phishing sites, network and device-wide monitoring, and email security tools that can identify suspicious messages and malicious links.
- Implement verification policies for payments, so multiple people have to approve an invoice before wiring funds, and that payments are only made via approved channels. Attackers will often require payments in methods that are hard to trace or block, including gift cards and cryptocurrencies.
- Reduce your attack surface by embracing the Zero Trust concept of "least privilege access". By ensuring employees have the least amount of access required to do their job (or, put another way, they can only access the tools and systems they need, and nothing else), you limit the potential damage from a successful phishing attack.
- Adopt next-generation identity technologies like passkeys that support passwordless and phishing-resistant user experiences with continuous threat protection.

okta
The World's Identity Company

Identity at the front line against phishing



A threat actor’s worst nightmare? Vigilant employees

Your workforce is your strongest protection against phishing attacks. Trained, tested, and vigilant employees — those unafraid to ask questions — are a threat actor’s worst nightmare. They can, collectively, stop a phishing attack in its tracks.

But it’s always good to have extra reassurance. Thousands of businesses rely on Okta to help protect their employees and customers from online threats. We make it easy to deploy modern Identity technologies like adaptive, phishing resistant MFA. Our Identity platforms play nice with the Identity Threat Detection and Response (ITDR) tools you already use, like Cisco Umbrella, Rootly, and others.

To find out more, reach out to an Okta rep here.

okta
The World's Identity Company

Thank you for reading

Ultimate guide to phishing