CyberSmart

What is phishing in cybersecurity?

Contents

Introduction

Phishing attacks are common and costly. Phishing exploits human psychology and preys on emotions like curiosity, urgency, and fear. It's the most prevalent type of cyberattack, and according to 61% of businesses is the most disruptive.

Here's what you need to know to keep your business safe.

What is phishing?

Phishing in cybersecurity is a type of social engineering attack where scammers use fake emails, texts, or websites to trick you into revealing sensitive data.

The most targeted industries for phishing are:

1. SaaS
2. Social media
3. Financial institutions
4. E-commerce/Retail
5. Payment

The evolution of phishing

Phishing was first coined in the mid-1990s to describe a group of scammers posing as employees and using email and instant messaging to steal login information and hijack accounts.

Three decades on, and what started as generic, poorly worded comms sent to groups of unsuspecting people has developed into well-researched, highly targeted attacks.

Technology is instrumental in shaping phishing tactics, while the rise of phishing-as-a-service (where hackers can access phishing kits, templates, and code) has lowered the barrier to entry. This makes it even easier for low-skilled scammers to launch convincing campaigns.

Now, there's another game-changer – AI.

The impact of AI on phishing

When you think about a phishing attack, your mind probably goes to messages full of typos, spelling mistakes, and strange requests.

But AI is a whole other kettle of fish. It enables cybercriminals to mimic natural language and tailor messages, making scams extremely difficult to spot.

What's more, AI's ability to generate diverse textual phrasing (varied language) means messages aren't flagged by spam filters.

For example, a subject line like "Get rich quick" is likely to be flagged, but AI might rephrase it as "Discover rapid income secrets," which is less likely to trigger filters.

Then there's deepfakes. Deepfakes are AI-generated videos, pictures, and audio clips made to look like real people. They're often used to impersonate politicians and celebrities and spread disinformation. However, they can also make phishing attacks close to impossible to detect.

Scammers used deepfakes for video calls to convince victims to share sensitive information or even money. There's one case where a Hong Kong employee was tricked into transferring £20 million to a scammer who used deepfake technology to pose as a senior official.

Although AI platforms, like ChatGPT, have rules in place to prevent misuse, getting around these restrictions is just a matter of creative prompting. Not to mention that cybercriminals have created custom GPTs, such as FraudGPT, WormGPT, and PoisonGPT.

Types of phishing attacks

Phishing attacks can take many forms and occur through various mediums. Common types of phishing include:

Spear Phishing

This is a targeted phishing attack that uses personal details to deceive specific individuals. HR executives and IT managers are popular targets for spear phishing because they have high levels of access. Before launching the attack, scammers gather as many details about the target as possible – from their manager's name to which bank they use. This makes the phishing messages appear legitimate.

Whaling

Whaling takes spear phishing a step further (or should we say deeper?) and targets the C-suite. Once scammers have successfully tricked the target, they use their details to trick other people and request fraudulent wire transfers.

The top 5 most targeted job titles for phishing are:

- CEO
- CFO
- CPO
- CISO
- CRO

Smishing

Smishing is a combination of the words SMS and phishing. It occurs when cybercriminals send fake texts to trick recipients into sharing confidential information, transferring money, or downloading malware. Smishing has gained traction with the rise of online shopping because it's common for companies to use SMS to update customers on their orders.

Pop-up phishing

Pop-up windows imitating legitimate sources, like software providers or banks, trick victims into sharing credentials.

Pop-up phishing can occur on both desktop and mobile devices and is commonly seen on compromised websites or through malicious advertisements.

SVG phishing

Scalable vector graphics (SVG) phishing uses an image file format to evade traditional security measures. This enables scammers to send emails containing dodgy attachments.

Quishing

Scammers use QR codes to send users to malicious websites. It's especially effective when codes are placed in credible places, like on retail products and branded marketing.

Vishing

Short for voice phishing, vishing involves fraudulent phone calls or voice messages that trick victims. In a typical vishing scam, fraudsters pose as representatives from trusted organisations like banks to manipulate targets into revealing sensitive information. However, the rise of generative AI has made these attacks even more convincing. Scammers can now use advanced voice cloning technology to imitate the voices of people you know and trust.

Angler phishing

Cybercriminals create fake social media profiles and accounts to pose as customer service agents and trick victims into sharing credentials. For example, a hacker replies to someone's complaint about a company on Facebook and asks them for their login details.

Watering-hole phishing

Scammers compromise an entire website, infecting anyone who visits it. A watering hole attack is highly targeted as scammers identify websites that users from specific organisations or sectors visit regularly.

Did you know?

About 1.2% of all emails are phishing attempts, adding up to around 3.4 billion malicious emails daily worldwide.

Notable phishing attacks

To see the real-world impact of phishing, here are a few high-profile attacks from recent years.

Pepco loses €15.5 million

In 2024, Pepco Group, which includes Pepco, Poundland, and Dealz brands, confirmed that its Hungarian business lost €15.5 million (£13 million) in a phishing attack. They believe the scammer spoofed a legitimate employee email address to trick other employees into processing payments.

Coinbase Smishing attack

Attackers used smishing to target cryptocurrency platform, Coinbase. They sent text messages to employees claiming to contain "important corporate notifications" that directed victims to fake login pages. Employee data was exposed, including names, email addresses, and phone numbers. However, multi-factor authentication prevented a full breach.

MGM Resorts international attack

The 'Scattered Spiders' hacker group used LinkedIn to identify an MGM employee, then called the IT help desk impersonating them. In a 10-minute phone call, they convinced support staff to grant administrator privileges to MGM's Okta and Azure environments. The attack caused approximately $100 million (£71.9 million) in damages.

M&S cyberattack

In February 2025, the DragonForce ransomware group infiltrated Marks and Spencer's systems after a successful social engineering attack. The attack caused online and in-store disruptions, resulting in £300 million in lost operating profit and over £1 billion in their stock market value. In addition, the attack compromised customer data, including names, addresses, phone numbers, birth dates, and purchase histories.

How to spot a phishing attack

Urgency or threats

Watch out for messages that say you must click, call, open, or make a payment immediately, employ some scepticism. Slow down and double-check what you've been asked to do.

Incorrect email domains

Always check the senders email address. Look for subtle misspellings or additions, for example gmail2.com or rnicrosoft.com.

Unexpected links and attachments

If you don't know what the attachment contains, don't open it. Hover your mouse over the link and look at the address that shows.

Generic details

Impersonal and generic greetings like "Dear customer" should raise a red flag. Legitimate organisations will have your name so they can address you directly.

With attacks becoming increasingly sophisticated, spotting phishing attempts is more challenging than ever. However, there are still some red flags to watch out for.

Inconsistencies

If you're suspicious about an email or text, always go back to the original source and contact the person directly from there. For example, if they say they're a customer service representative for a brand, go to the brand's website and access their customer support that way.

You can also check details like email addresses against what's listed on the official website.

Unprompted login requests

Only enter login details to a site you've navigated to by yourself or requested a login code for.

Glitches

Deepfake videos can look incredibly realistic, but watch for unnatural facial movements, awkward voice sync, or blurry edges.

If you receive a video message out of the blue, verify it through another channel.

Ready to level up your phishing defences?

Put your knowledge into action with CyberSmart Learn – easy, expert-led training designed to keep your team one step ahead of cyber threats.

Learn more

FAQs

How to prevent phishing?

- Implement robust email filters and anti-malware software
- Train employees to recognise and report phishing red flags
- Establish clear protocols for handling sensitive data and financial requests
- Use multi-factor authentication on all accounts
- Keep all systems and software up-to-date with the latest security patches
- Regularly back up critical data in case of a breach

What should I do if I suspect a phishing attempt?

If you think a message is suspicious, don't click any links, open attachments, or provide personal information. Flag the message as spam or junk. If it appears to come from a known contact, reach out to them through a different channel to verify. You should also alert your IT department or managed service provider right away.

How can I tell if a website is legitimate?

Before entering any sensitive data into a website, check that the URL begins with "https" rather than just "http" – this indicates a secure connection. Also, look for a lock icon next to the URL. Be wary of sites with misspellings, low-quality images, or unprofessional designs. When in doubt, navigate to a site directly rather than clicking email links.

What type of phishing is most difficult to detect?

Spear phishing attacks are often the hardest to spot. Unlike 'spray and pray' mass phishing emails, spear phishing is highly targeted. The attacker researches their victim and crafts a personalised message based on that individual's job, interests, or contacts.

These emails come from a trusted sender and look legitimate, making them tough to distinguish from genuine messages. They rarely set off spam filters, as they're not bulk emails. Without careful scrutiny, even savvy users can fall for a spear phishing scam.

Who sends phishing emails?

Phishing emails can come from various sources, but common culprits include:

- Hackers: people who get a thrill from breaking into systems and causing disruption. While their motives aren't always financial, their methods can be just as damaging.
- Insiders: rogue employees or contractors who misuse their access to company systems. They may have an axe to grind or be working with outside criminals.
- Nation states: some phishing attacks are part of state-sponsored espionage or sabotage campaigns. These attackers are highly sophisticated and persistent.