Phishing Awareness

Cloud Destinations

Embrace Cloud Multiverse

What Is Phishing?

Phishing is a form of fraud in which an online attacker, usually impersonating a trusted source, influences a victim to disclose sensitive information, or click a harmful link.

The motive of launching a phishing scam can range, although financial gain, data theft and even competitive advantage are often the cause.

How Does It Work?

Phishers use a range of tools to reach out to their victims, including text messages, social media and mobile phones are all options for an attacker, although email is undoubtedly the most popular weapon of choice.

Many of these scams are emailed in a "spray and pray" approach, with generic email templates sent out in their masses in the hope of tricking a number of unsuspecting users.

Social engineering and pretexting techniques offer much more personalised techniques of attack - with prior research of a victim being used in order to add some extra layers of knowledge and trust in the eyes of an unsuspecting victim.

Why Is Phishing So Successful?

- A lack of employee awareness training
- Increasingly sophisticated techniques
- More personalised campaigns
- The widespread availability of phishing tools

No awareness?

97%

The percentage of people around the world unable to identify a **sophisticated** phishing email

12%

The percentage of users who **click the link** after opening a malicious email.

Cloud Destinations

Embrace Cloud Multiverse

The Most Common Types Of Employee Phishing

Email Phishing: The original.

This scam often relies heavily on a 'spray-and-pray' approach, where fraudulent emails are sent in their masses to a large number of recipients.

These emails often impersonate a known or trusted company or individual, with the aim of tricking a person into parting ways with personal information - whether that be login credentials or banking information. Attacks can also encourage an unsuspecting user to download a harmful email attachment or a file from a fake website - opening the door to a damaging malware infection.

All of this is made possible by what's known as 'email spoofing', where email headers and subject lines are forged to make the email look as legitimate as possible. Huge organisations such as Apple and Microsoft are often spoofed in these attacks, due to their huge number of users and trusted reputation.

Spear Phishing: Time to get personal.

Not all phishing scams are generic. 'Spear phishing' fraudsters customise their attack emails to contain the target's name, company, position, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender.

Spear phishing is especially popular on social media sites like LinkedIn, where attackers have a range of useful information.

Whaling: There's always a bigger phish.

In another scam involving the bigger fish of the organisation, a whaling attack targets only an organisation's top executives. The term whaling reflects exactly this - with a cyber criminal not wanting to waste time on smaller fish and, instead, targeting the 'whales' of the company due to the value of information they hold.

Prior research is also important for the criminal here, with social engineering techniques being deployed in order to obtain information that can later be used in the phishing email.

BEC/ CEO Fraud: The art of impersonation.

In this increasingly common phishing scam, attackers can compromise the email account of a high-level exec or financial officer via an already successful spear phishing attack, or previous infection. The criminal then patiently spies on the account's email activity, while gathering valuable information on processes and procedures of the business.

When equipped with enough information to effectively impersonate the executive, the attacker will send an email - usually containing urgency or high importance - and requests that the victim transfer funds to a specified account. Sure, it's a riskier scam, yet still a lucrative favourite in the world of cyber crime.

Cloud Destinations
Embrace Cloud Multiverse

How To Spot The Red Flags Of A Phish

#1. Mismatched URLs:

Often, the embedded URL in a phishing message will appear to be perfectly valid, but when hovering your mouse over the URL, the actual hyperlinked address may appear differently. This is an indicator that the link could be fraudulent.

#2. Poor Spelling/ Grammar:

Large companies often have strict processes in place for reviewing company messages, especially when it comes to grammar, spelling and legality. So if you receive a message littered with mistakes, there's a chance it may not be from a legitimate source.

#3. Requesting Personal Info:

No matter how legitimate or official an email looks, it's always a suspicious sign when they ask you for personal information. Banks and reputable companies will never ask you to send account or credit card numbers, as they should already know these details.

Others To Look Out For:

- Special offers that sound too good to be true
- 'Responses' from companies you've never contacted
- URLs containing a misleading domain name
- Unrealistic threats, like having your account deleted
- Emails that contain attachments/ website links
- Messages that urge you to act quickly

Tricky subjects.
The Top 10.

The most common words in **BEC phishing** email subject lines.

Rank	Subject Line	%
#1	"payment"	13.8
#2	"urgent"	9.1
#3	"request"	6.7
#4	"attention"	6.1
#5	"important"	4.8
#6	"confidential"	2.0
#7	"immediate response"	1.9
#8	"transfer"	1.8
#9	"Important update"	1.7
#10	"attn"	1.5

Cloud Destinations

Embrace Cloud Multiverse

- Clearly assess user vulnerability
- Give users real-world experience of an attack
- Determine where education is most needed
- Demonstrate the need for security training budget

.

-17%

The average decrease of users who give away **account credentials** during a second phishing simulation.