

PHISHING AWARENESS TRAINING

Be Aware and Do Not Take the Bait!





Table of contents

01 What is Phishing?


This section will peel back the layers of deception used in phishing attacks, focusing on the psychological manipulation tactics known as social engineering.

03 Social Engineering Tactics

This section serves as the foundation of the presentation, shedding light on the deceptive world of phishing.

05 What to Do If You Fall Victim

This section addresses a crucial aspect: what actions to take if someone accidentally falls for a phishing attempt.




02 The Anatomy of a Phishing Attempt

This section will delve deeper into the inner workings of a phishing attack, dissecting the typical steps phishers take to deceive their victims.

04 How to Protect Yourself

This section empowers your audience by equipping them with practical strategies to defend themselves against phishing attempts.

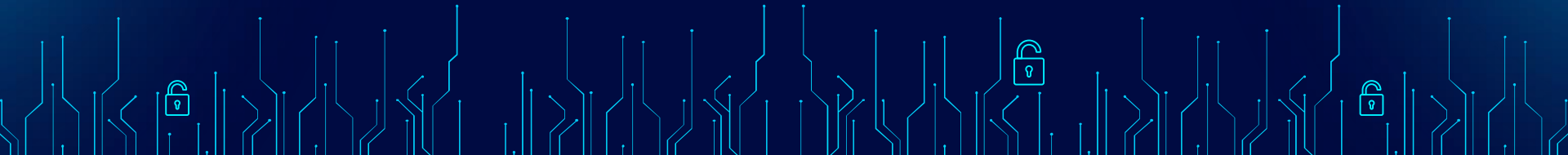




Raise your hand if you've ever received an email that seemed a little too good to be true, maybe promising a free vacation or a sudden inheritance from a long-lost relative. Pause for audience response Well, you're not alone. These are classic examples of phishing attempts, and unfortunately, they're becoming increasingly sophisticated.

01

What is Phishing?





What is Phishing?

Phishing is a sneaky attempt by criminals to trick you into giving away personal information, like passwords or credit card numbers. They often do this by sending emails or text messages that look like they're from a real company, like your bank or a store you shop at. These messages will try to scare you or create a sense of urgency so you rush to click on a link or open an attachment.

Methods of Phishing

Email Phishing

This is the most widespread method. Phishers send emails disguised as legitimate sources like banks, credit card companies, popular online services (e.g., Netflix, Dropbox), or even your IT department.

Smishing

Phishing attempts via SMS text messages. Phishers may use similar tactics as email phishing, creating a sense of urgency and using link shorteners to disguise malicious URLs.

Methods of Phishing

Vishing

Phishing attempts via phone calls. The caller might impersonate someone from a trusted organization (e.g., bank, tech support) and try to trick you into revealing personal information or downloading malware.

Spear Phishing

A more targeted approach where phishers tailor emails to a specific individual. They might gather information from social media profiles or data breaches to personalize the email content and increase its legitimacy

Methods of Phishing

Clone Phishing

Involves sending a near-identical copy of a legitimate email you previously received. For instance, if you recently received a shipment notification email, the phisher might send a copy with a malicious attachment

Watering Hole Phishing

Targets a specific group of people by compromising websites they are likely to visit. Once a user visits the compromised site, they are redirected to a malicious website designed to steal information.

Angler Phishing

Leverages social media platforms to spread phishing attacks. Phishers might create fake social media profiles or exploit vulnerabilities to post malicious links or encourage clicks to fake websites

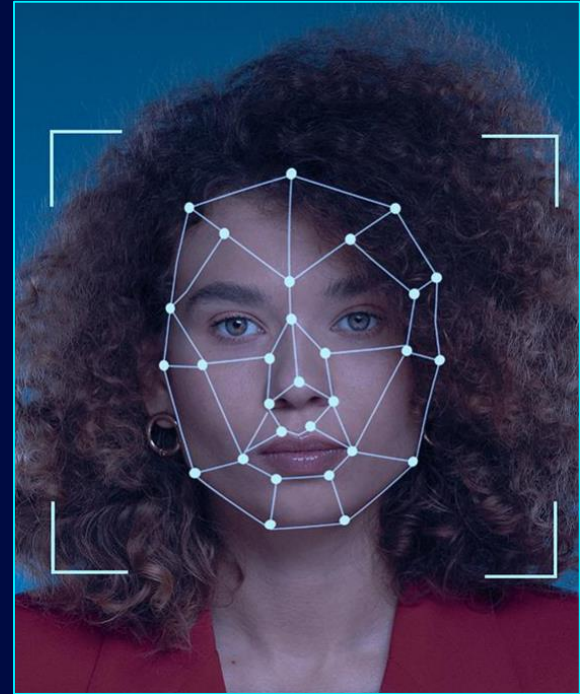
The impact of phishing For Individuals:

Identity Theft

Phishing attacks often target personal details like usernames, passwords, Social Security numbers, or addresses. If successful, phishers can use this stolen information to commit identity theft, opening new accounts, taking out loans, or making fraudulent purchases in your name. This can lead to significant financial losses and damage to your credit score.

Financial Loss

Gaining access to your bank accounts or credit card information is a primary goal for phishers. Once they have this information, they can steal your money directly through unauthorized transactions.



The impact of phishing For Individuals:

Data Loss

Phishing attacks can be used to install malware on your device. This malware can steal sensitive data stored on your device or give phishers remote access to your system.

Emotional Distress

Dealing with the aftermath of a phishing attack can be stressful and time-consuming. You may need to cancel compromised accounts, report fraud, and restore your identity.



The impact of phishing For Organizations:

Data Breaches

Phishing attacks are a leading cause of data breaches. If an employee falls victim to a phishing scam, it can give attackers access to a company's network and sensitive data, exposing customer information, financial records, or intellectual property.

Financial Losses

Data breaches can be incredibly expensive for organizations, with costs associated with remediation, regulatory fines, and lawsuits.



The impact of phishing For Organizations:

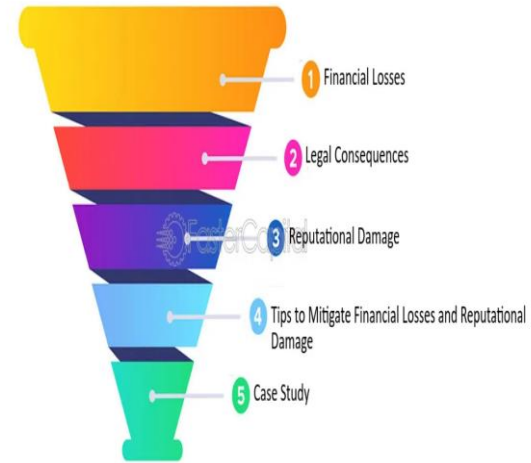
Reputational Damage

A data breach can severely damage an organization's reputation. Customers may lose trust and take their business elsewhere.

Financial Losses

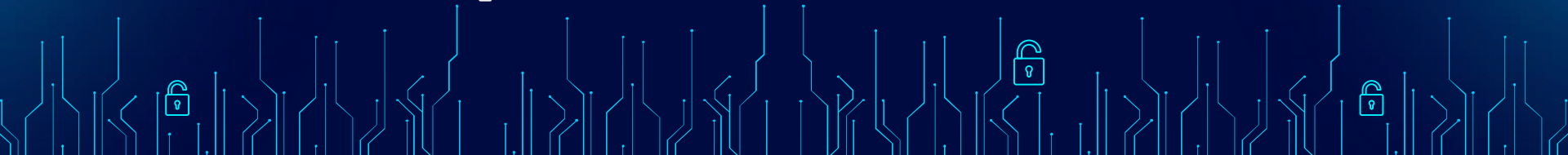
Data breaches can be incredibly expensive for organizations, with costs associated with remediation, regulatory fines, and lawsuits.

Financial Losses and Reputational Damage



02

The Anatomy of a Phishing Attempt







Phishing Email

From: mastercardsIT@gmail.com
To: employee@email.com
Subject: URGENT! Password Reset Required

—

Body:

Hello (insert name) ,

Your email account has been compromised. immediate action is required to reset your password!

Click here to reset your password in the next hour or your account will be locked:

<https://en.wikipedia.org/wiki/Phishing>

Regards,
Mastercard IT



**This is one example of an improved phishing email.
There are many different ways you could have done this.**

Spelling of Mastercard fixed and email comes from a relatable address

From: Mastercard Staff Rewards

To: employee@email.com

Subject: Your Black Friday Employee reward card

Body:

Hello <name>,

Email is personalized and poor grammar is fixed

Contextualize to upcoming Black Friday event

In recognition of your hard work throughout the year, we wish to reward you with a gift card to spend in the upcoming **Black Friday** sales as a small token of our appreciation. Please find attached your Employee reward card.

Link is masked in plaintext to hide phishing link

The balance of your card will be determined based on your role. To view the balance and activate your employee reward card, visit [here](#).

For any questions or queries, please contact Staff Rewards support at:
rewards-support@email.com

To increase legitimacy, buffer text is added

From,
Staff Reward Services

CONFIDENTIAL: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Simple confidentiality disclaimer to add legitimacy to email.
This was taken from an article on Exclaimer.com



Anatomy of Phishing Emails

**Subject Line (The
Attention Grabber)**

**Sender Address (The
Fake Facade)**

**Links and
Attachments (The
Phishing Traps)**


**Greeting (The Generic
Approach)**

**Email Body (The
Deceptive Disguise)**







Anatomy of Phishing Emails




The subject line is the **phishing email's headline**. It's designed to grab your attention and trick you into opening the email. Phishers use urgency, fake legitimacy, tempting offers, and personalization to make their subject lines seem important or interesting. Be wary of anything that seems too good to be true, and always double-check the sender before opening.



The sender address is the email's **disguised sender**, often spoofed to look like a trusted source like your bank or colleague. Be cautious of addresses that mimic real ones with typos or slight variations, and avoid generic senders. Always check carefully and verify legitimacy directly if unsure.



The greeting in a phishing email is the **generic welcome mat**. Phishers use impersonal greetings like "Dear Customer" or skip one altogether to target more victims and avoid detection. This lack of personalization is a red flag, so be cautious if an email claiming to be from someone you know uses a generic greeting.



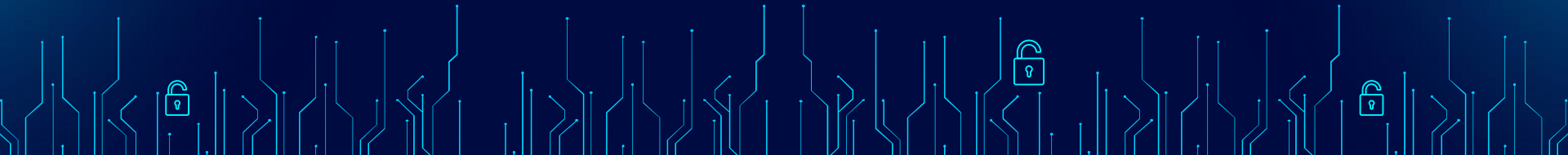
Anatomy of Phishing Emails

■ The email body is the phishing attempt's **deceitful costume**. Phishers use urgency, fear, or mimicked content to create a believable story. They aim to steal your information by tricking you into clicking links, downloading attachments, or revealing personal details. Be alert for these tactics and don't be afraid to delete suspicious emails and verify information directly.

■ Links and attachments are the **phishing email's hidden hooks**. They lure you in but deliver danger. Clicking suspicious links takes you to fake websites that steal your information, while attachments can contain malware that infiltrates your device. Always avoid these and verify legitimacy before clicking or opening anything.

03

Social Engineering Tactics



The Bait and Switch: Social Engineering in Phishing

Phishing attacks aren't just about technical trickery; they're a masterclass in manipulation. Here's how phishers exploit **social engineering tactics** to turn their emails into believable cons:



The Bait and Switch: Social Engineering in Phishing

The Trusted Disguise

Phishers masquerade as familiar faces - banks, credit card companies, even colleagues. Logos, layouts, and mimicked writing styles create a false sense of security, making you more likely to let down your guard.

Urgency and Fear: The One-Two Punch

Phishing emails play on emotions. They might warn of urgent account issues, expiring offers, or dire consequences for inaction. Panic clouds judgement, making you more likely to click that link without thinking.



The Bait and Switch: Social Engineering in Phishing

Curiosity's Siren Song:

Some phishers dangle irresistible offers or prey on your curiosity. Subject lines like "Congratulations! You've Won!" or "Exclusive Discount Inside" can pique your interest and lure you into the trap.

The Personal Touch (Spear Phishing):

In a more targeted approach, phishers might personalize emails with your name or reference specific details, making them appear even more legitimate.



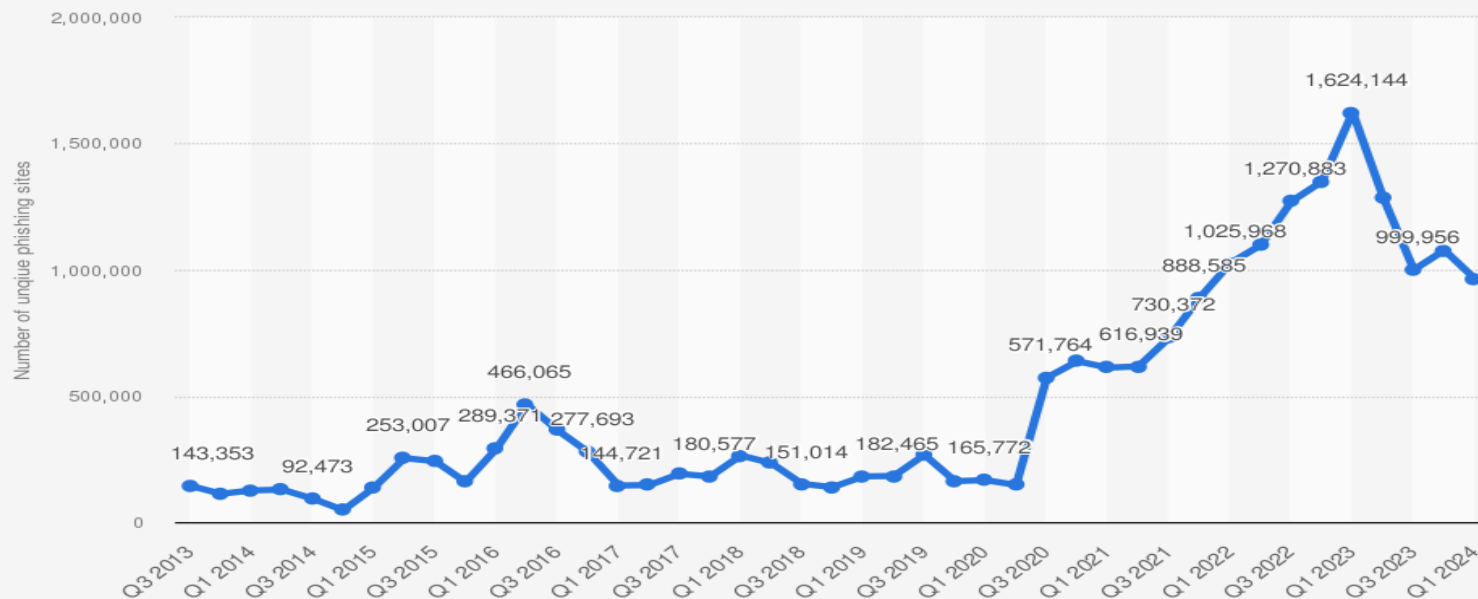
The Bait and Switch: Social Engineering in Phishing

By understanding these social engineering tactics, you become a shield against phishing scams. Remember, if something seems too good to be true, it probably is. Always be cautious and verify information directly with the supposed sender before taking any action.





Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 1st quarter 2024

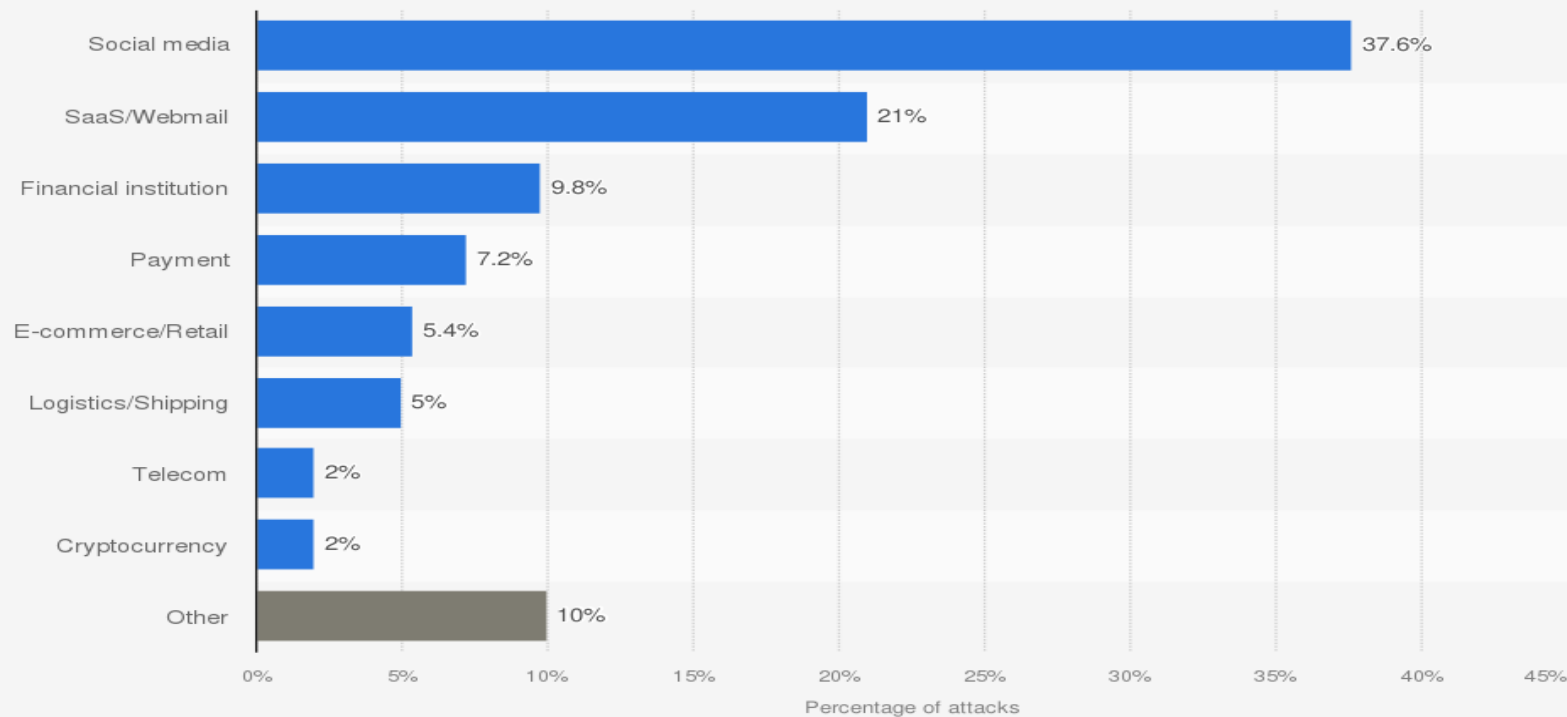


Source
APWG
© Statista 2024

Additional Information:
Worldwide; APWG; Q3 2013 to Q1 2024; based on APWG observations; wider industry metrics may vary



Online industries worldwide most targeted by phishing attacks as of 1st quarter 2024

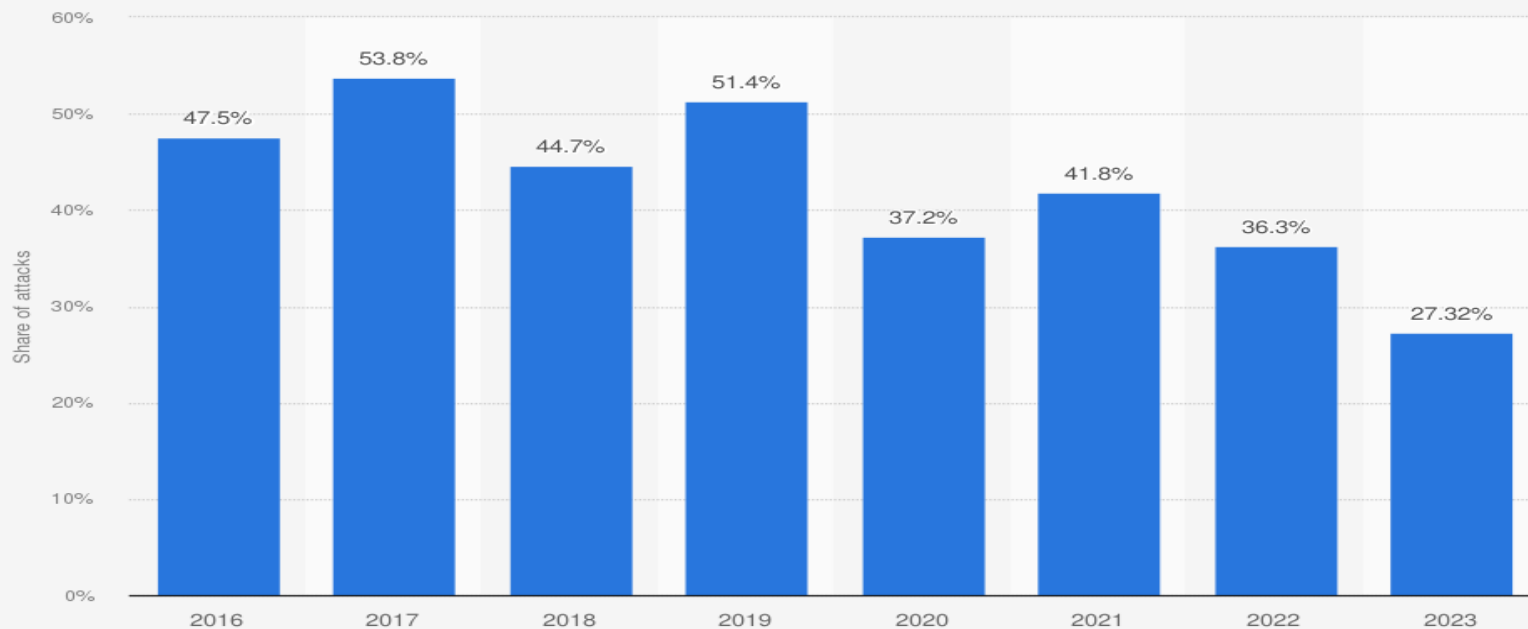


Source
APWG
© Statista 2024

Additional Information:
Worldwide; APWG; Q1 2024



Share of financial phishing attacks worldwide from 2016 to 2023



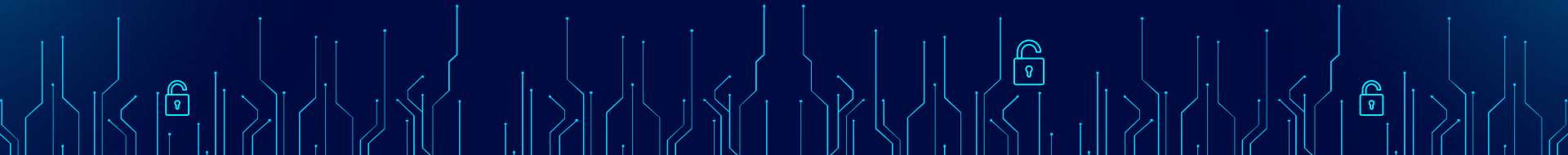
Source
Kaspersky Lab
© Statista 2024

Additional Information:
Worldwide; Kaspersky Lab; 2023; attacks detected by Kaspersky Labs, wider industry metrics may vary



04

How to Protect Yourself



Shielding Yourself: How to Outsmart Phishing Attempts

Phishing attacks may seem sophisticated, but with a few key strategies, you can significantly reduce your risk of falling victim. Here's your defense toolkit:

- 1. Become a Skeptic:** Don't trust everything you see in your inbox. Be wary of emails with a sense of urgency, unexpected attachments, or generic greetings.
- 2. Verify, Don't Click:** Never click on links or open attachments from suspicious emails. If you're unsure about a sender, verify their legitimacy by contacting them directly through a trusted channel (not by replying to the email).
- 3. Check the Sender Address:** Scrutinize the sender's email address carefully. Look for typos, misspellings, or slight variations of legitimate addresses.
- 4. Hover Over Links (Without Clicking):** Most email platforms allow you to hover your mouse over a link to see the actual destination URL before clicking. This can reveal a fake website disguised behind seemingly legitimate text.



Shielding Yourself: How to Outsmart Phishing Attempts

Phishing attacks may seem sophisticated, but with a few key strategies, you can significantly reduce your risk of falling victim. Here's your defense toolkit:

5. Beware of Phishing Lures: Don't be swayed by urgency, fear, or tempting offers. If something seems too good to be true, it probably is.

6. Fortify Your Passwords: Use strong, unique passwords for all your online accounts. Avoid using the same password for multiple accounts. Consider using a password manager to help you create and manage complex passwords.

7. Enable Multi-Factor Authentication (MFA): This adds an extra layer of security to your accounts by requiring a second verification step beyond your password when logging in.

8. Keep Software Updated: Ensure your operating system, web browser, and security software are updated with the latest security patches. Updates often include fixes for vulnerabilities that phishers can exploit.



Shielding Yourself: How to Outsmart Phishing Attempts

Phishing attacks may seem sophisticated, but with a few key strategies, you can significantly reduce your risk of falling victim. Here's your defense toolkit:

9. Report Phishing Attempts: If you encounter a phishing email, report it to your email provider and the appropriate authorities. This helps them track phishing campaigns and take action against them.

10. Educate Yourself: Stay informed about the latest phishing tactics. Many reliable sources offer educational resources on how to identify and avoid phishing scams.



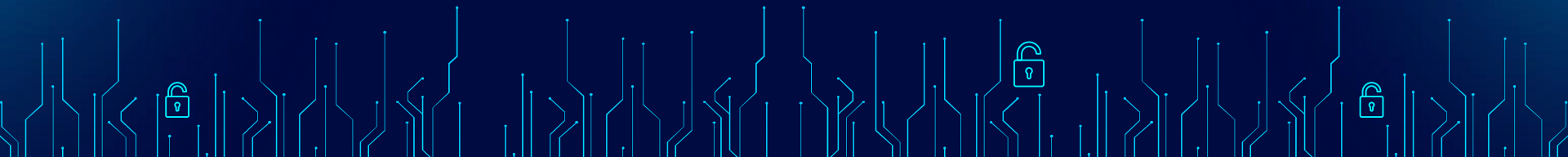
Shielding Yourself: How to Outsmart Phishing Attempts

By following these steps, you can significantly reduce your risk of falling victim to phishing attempts. Remember, vigilance is key. If something looks suspicious, it probably is. Don't hesitate to delete the email and verify information directly with the supposed sender.



05

What to Do If You Fall Victim



The Phishing Net: What to Do If You Fall Victim

Even the most cautious can fall prey to a well-crafted phishing attempt. Here's what to do if you suspect you've been phished:

- 1. Act Swiftly:** The faster you react, the better chance you have of minimizing the damage.
- 2. Change Your Passwords (Immediately!):** Start by changing the passwords for all your online accounts, especially those associated with the compromised email. Use strong, unique passwords and consider a password manager for better security.
- 3. Contact Your Financial Institutions:** If you suspect your financial information has been compromised, immediately contact your bank, credit card company, or any other relevant financial institution. Explain the situation and request to freeze your accounts or change your login credentials.
- 4. Secure Your Device:** If you clicked a suspicious link or opened an attachment, run a full scan with your antivirus software to detect and remove any potential malware.



The Phishing Net:

What to Do If You Fall Victim

Even the most cautious can fall prey to a well-crafted phishing attempt. Here's what to do if you suspect you've been phished:

- 5. Report the Phishing Attempt:** Reporting the phishing attempt helps authorities track these scams and take action against perpetrators. Report the email to your email provider and consider reporting it to relevant anti-phishing organizations (resources on next slide).
- 6. Monitor Your Accounts:** Keep a close eye on your financial statements and account activity for any suspicious transactions. Report any unauthorized activity to your financial institutions immediately.
- 7. Learn from the Experience:** Take this as a learning opportunity. Analyze what made you susceptible to the phishing attempt and use it to strengthen your defenses in the future.



Resources for Reporting Phishing Attempts



The Phishing Net:

What to Do If You Fall Victim

Include logos and links to relevant organizations in your area that accept phishing reports. Here are some examples:

1. [Anti-Phishing Working Group \(APWG\)](#)
2. [Federal Trade Commission \(FTC\)](#)
3. [National Cyber Security Alliance \(NCSC\) - UK](#)

By following these steps, you can take control of the situation and minimize the damage caused by a phishing attack. Remember, reporting these attempts helps create a safer online environment for everyone.



Thanks!

Any questions?

elsayedrezkallah1@gmail.com
+20 106 046 6759

