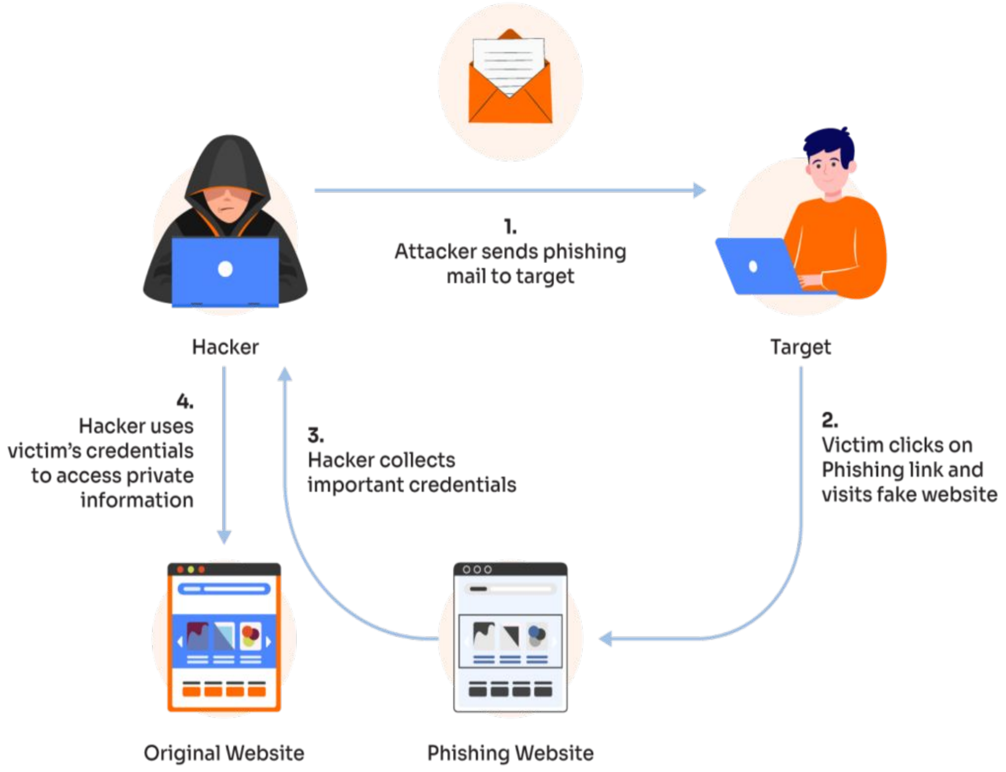
Phishing Awareness Training

Introduction to Phishing

Phishing is a form of cyberattack that aims to trick individuals into providing sensitive information.

These attacks often come in the form of emails or messages that appear legitimate.

Understanding phishing is crucial to protecting personal and organizational data.

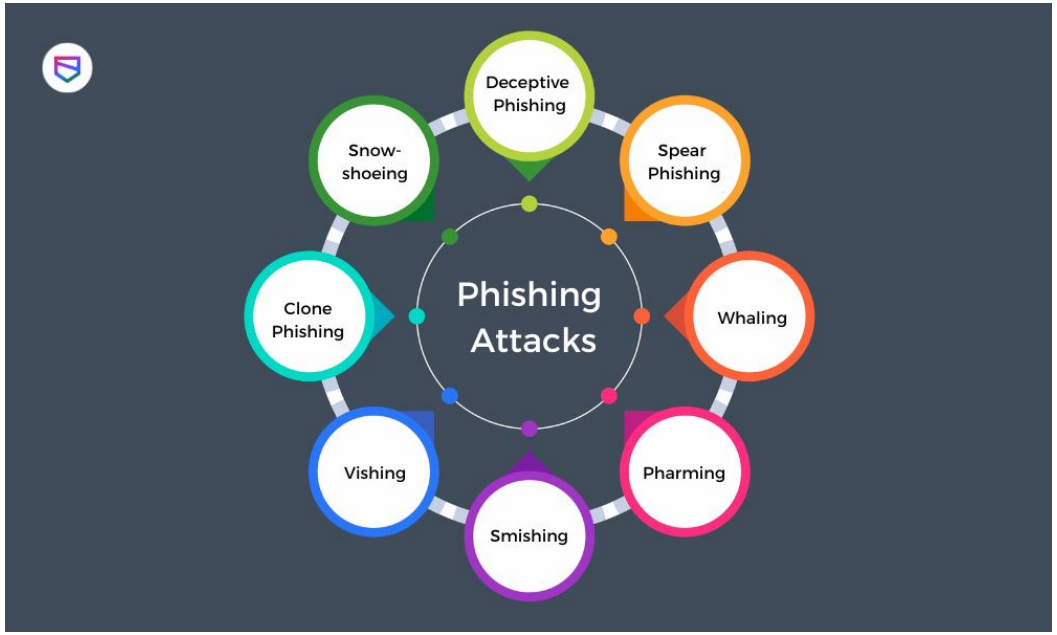

1.
Attacker sends phishing mail to target
Hacker
Target
2.
Victim clicks on Phishing link and visits fake website
3.
Hacker collects important credentials
4.
Hacker uses victim's credentials to access private information
Original Website
Phishing Website

Types of Phishing Attacks

Phishing can take various forms, including email phishing, spear phishing, and whaling.

Email phishing targets a broad audience, while spear phishing is directed at specific individuals.

Whaling attacks are aimed at high-profile targets, such as executives or important figures.

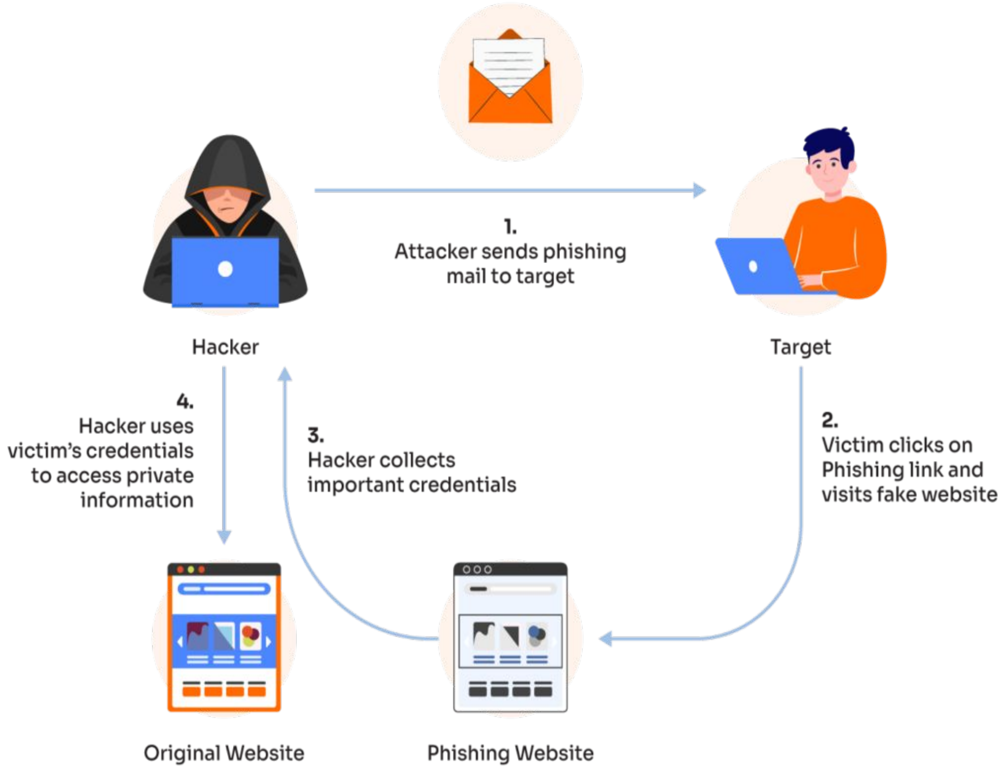


How Phishing Works

Attackers often create counterfeit websites to capture user credentials.

They use social engineering techniques to create a sense of urgency or fear.

Phishing emails usually contain links or attachments that can lead to malware installation.



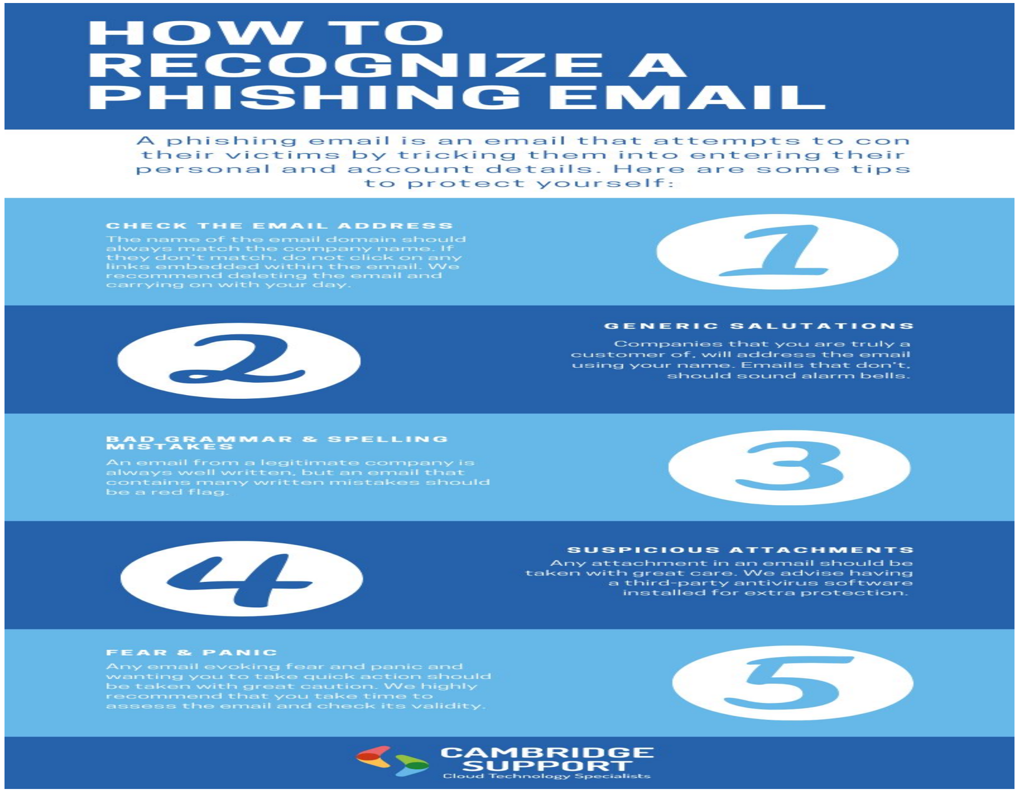
1.
Attacker sends phishing mail to target
Hacker
Target
4.
Hacker uses victim's credentials to access private information
3.
Hacker collects important credentials
2.
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

Recognizing Phishing Emails

Look for generic greetings or misspellings that can indicate a phishing attempt.

Be cautious of emails requesting urgent action or personal information.

Always verify the sender's email address for authenticity before clicking any links.



HOW TO RECOGNIZE A PHISHING EMAIL

A phishing email is an email that attempts to con their victims by tricking them into entering their personal and account details. Here are some tips to protect yourself:

1

CHECK THE EMAIL ADDRESS

The name of the email domain should always match the company name. If they don't match, do not click on any links embedded within the email. We recommend deleting the email and carrying on with your day.

2

GENERIC SALUTATIONS

Companies that you are truly a customer of, will address the email using your name. Emails that don't, should sound alarm bells.

3

BAD GRAMMAR & SPELLING MISTAKES

An email from a legitimate company is always well written, but an email that contains many written mistakes should be a red flag.

4

SUSPICIOUS ATTACHMENTS

Any attachment in an email should be taken with great care. We advise having a third-party antivirus software installed for extra protection.

5

FEAR & PANIC

Any email evoking fear and panic and wanting you to take quick action should be taken with great caution. We highly recommend that you take time to assess the email and check its validity.

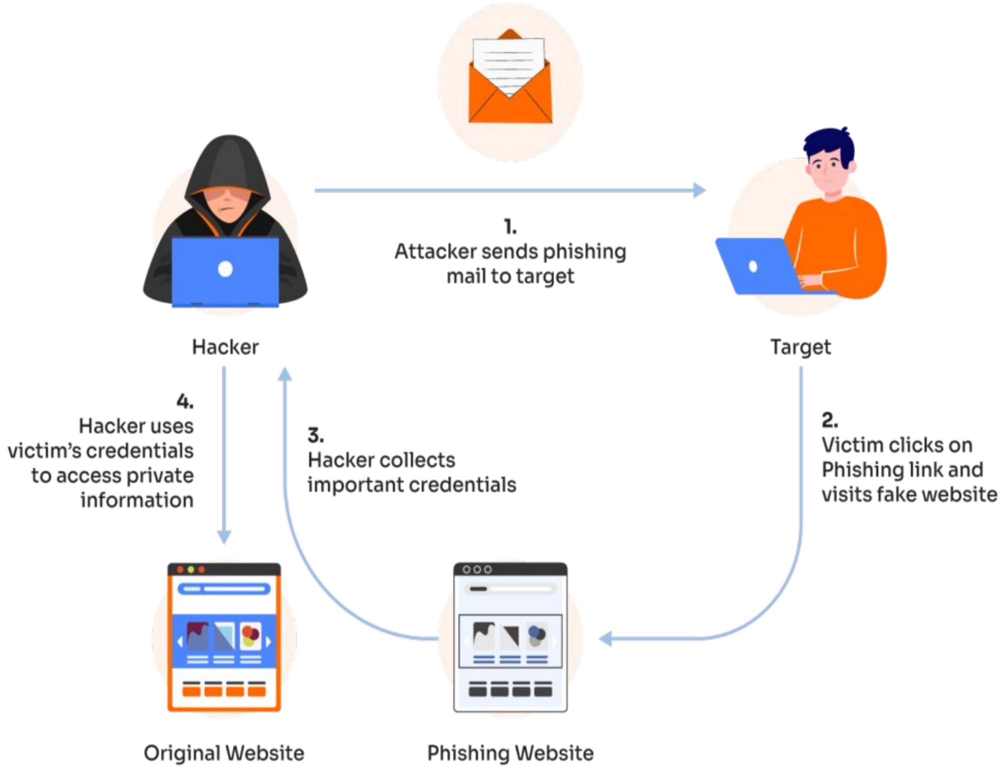
CAMBRIDGE SUPPORT
Cloud Technology Specialists

Common Phishing Techniques

Attackers often impersonate reputable organizations to gain trust.

They may create fake websites that closely resemble legitimate ones.

Spoofing email addresses is a common tactic to trick recipients into believing the source is genuine.



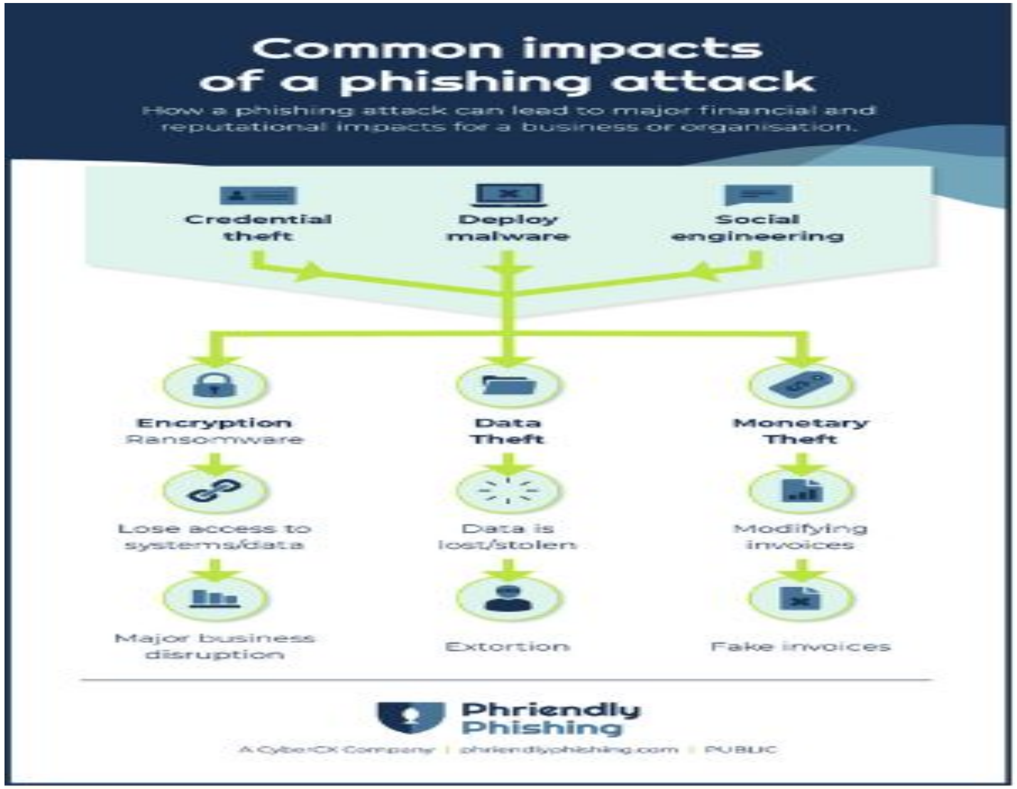
Hacker
Target
1. Attacker sends phishing mail to target
2. Victim clicks on Phishing link and visits fake website
3. Hacker collects important credentials
4. Hacker uses victim's credentials to access private information
Original Website
Phishing Website

The Consequences of Falling for Phishing

Falling victim to phishing can lead to identity theft and financial loss.

Organizations may suffer data breaches, leading to loss of customer trust and legal issues.

Infected systems can be used to launch further attacks, creating a ripple effect.

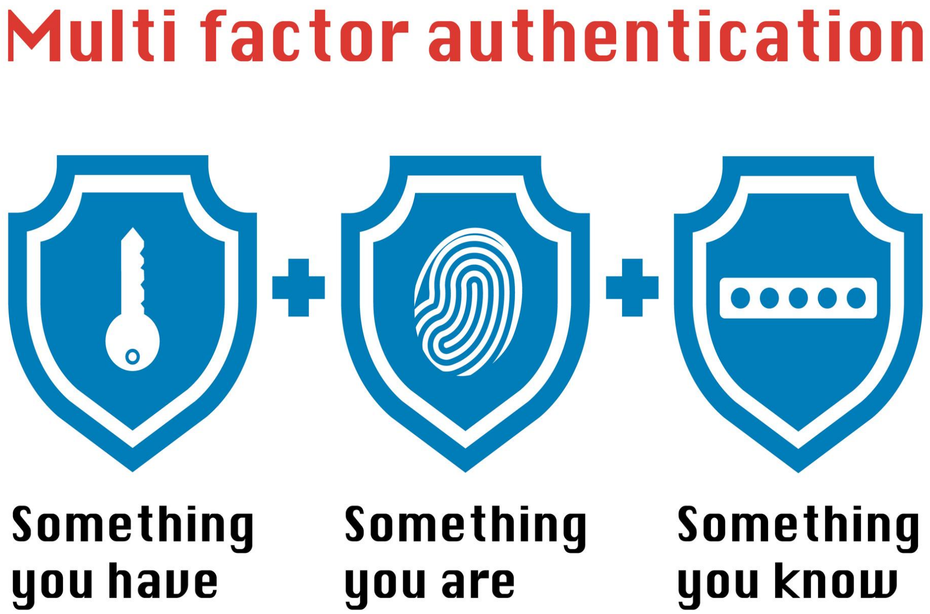

Common impacts of a phishing attack
How a phishing attack can lead to major financial and reputational impacts for a business or organisation.
Credential theft
Deploy malware
Social engineering
Encryption Ransomware
Data Theft
Monetary Theft
Lose access to systems/data
Data is lost/stolen
Modifying invoices
Major business disruption
Extortion
Fake invoices
Phriendly Phishing
A CyberCX Company | phriendlyphishing.com | PUBLIC

How to Protect Yourself

Use multi-factor authentication wherever possible to add an extra layer of security.

Regularly update passwords and use unique passwords for different accounts.

Keep software and security systems up to date to protect against vulnerabilities.



Reporting Phishing Attempts

Always report suspicious emails to your IT department or designated authority.

Many organizations have protocols for reporting phishing attempts to increase awareness.

Reporting helps in tracking and mitigating potential threats to the entire organization.

Received a suspicious email?
• Spot red flags.
• Report and delete.
• Prevent.

Best Practices for Organizations

Conduct regular phishing awareness training for all employees.

Encourage a culture of security where employees feel comfortable reporting suspicious activity.

Implement comprehensive security measures, including email filtering and anti-phishing tools.

Z CYBERSECURITY
CONTENT . SOCIAL . MARKETING

Phishing Safety Tips

Think before you click

Always be wary of emails, links, and attachments from unknown or suspicious sources.

Use a secure VPN connection.

A Virtual Private Network (VPN) will ensure your anonymity on the internet.

Be careful of what you post.

Remember: what you post on the internet will stay there forever.

Practice safe browsing.

A single careless click can expose your sensitive information. Think before you click!

Be careful of what you download.

Avoid downloading apps or software that look suspicious. It may result in malware.

Stay safe online!

Conclusion and Resources

Staying informed is the first step in protecting against phishing attacks.

Utilize available resources such as cybersecurity newsletters and awareness programs.

Continuous education and vigilance are key to minimizing the risk of phishing attacks.