Cybersecurity
PHISHING AWARENESS TRAINING

Key Objectives:

- Understand what phishing is and how it works
- Recognize different types of phishing attacks
- Learn best practices for avoiding phishing scams
- Know the steps to take if you encounter a phishing attempt

Agenda:

- Introduction to Phishing
- Common Phishing Techniques
- Real-Life Examples
- Best Practices for Prevention
- Reporting Phishing Attempts

Presented by

Afifa Iqbal

- MSc (Math) (Riphah International University)
- CEH (UNIVERSITY OF LAHORE)

Experience
Teaching (2019-2022)
Graphic Designing (2021-2023)

Contact # +923055858863
EMAIL # afifaiqbal00@gmail.com

Phishing

Phishing is a type of online fraud where individuals or groups deceive internet users, aiming to trick them into revealing sensitive or confidential information.

What is a phishing attack?

A phishing attack involves misleading a victim into performing actions that benefit the attacker. These attacks vary in complexity and can be identified with proper awareness.

Typically, attackers send fake links or emails to steal personal data from the victim’s device. Common phishing techniques include:

- Fake emails
- Spam messages
- Social media scams

Staying alert can help prevent falling for these fraudulent tactics.

Definitions

Phishing is a technique used to obtain sensitive data, such as bank account details, by sending fraudulent emails or creating fake websites. In these attacks, the perpetrator pretends to be a trusted business or reputable individual to deceive victims into sharing their personal information.

- **Sources:**
  CNSSI 4009-2015 from IETF RFC 4949 Ver 2
  NIST SP 800-12 Rev. 1 under Phishing from IETF RFC 4949 Ver 2
- Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
  Sources:
  NIST SP 800-150 under Phishing from NIST SP 800-88 Rev. 1
  NIST SP 800-45 Version 2 under Phishing
  NIST SP 800-83 Rev. 1 under Phishing
- A digital form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake Web site that requests information.
  Sources:
  NIST SP 800-115 under Phishing
- Using social engineering techniques to trick users into accessing a fake Web site and divulging personal information.
  Sources:
  NIST SP 800-44 Version 2 under Phishing

How Phishing Attacks Happen

Phishing occurs when a victim responds to a fake email that urges quick action. Common actions requested in phishing emails include:

- Clicking on a harmful attachment
- Enabling macros in documents
- Updating passwords
- Responding to fake social media requests
- Connecting to malicious Wi-Fi

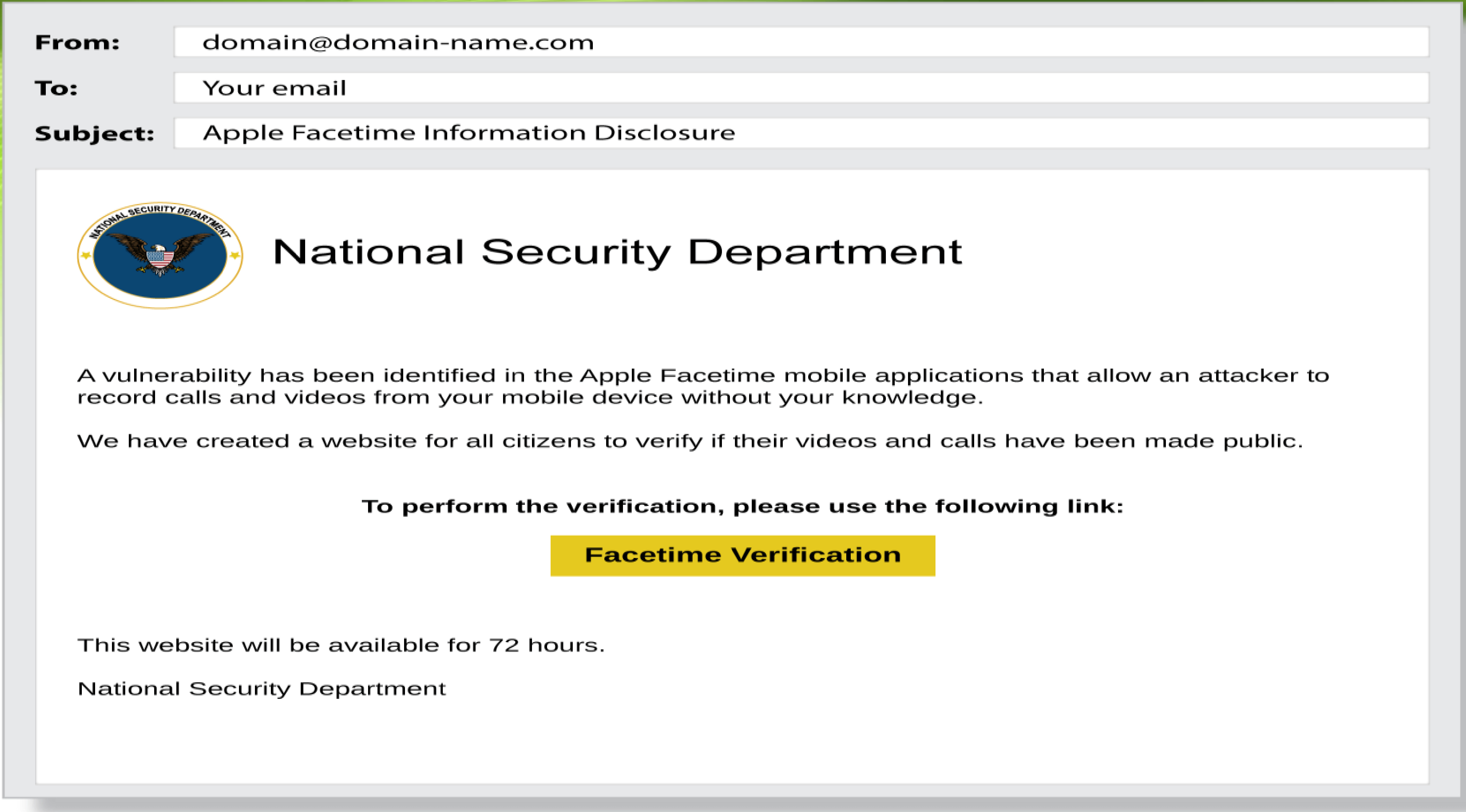
Cybercriminals constantly improve their tactics, using phishing through emails, texts, and voicemails.

Real-World Phishing Examples

Phishing emails use social engineering to exploit trust in people or organizations. Victims often:

- Transfer funds
- Share login details
- Give access to sensitive data

These tactics make phishing highly effective in deceiving individuals.



From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

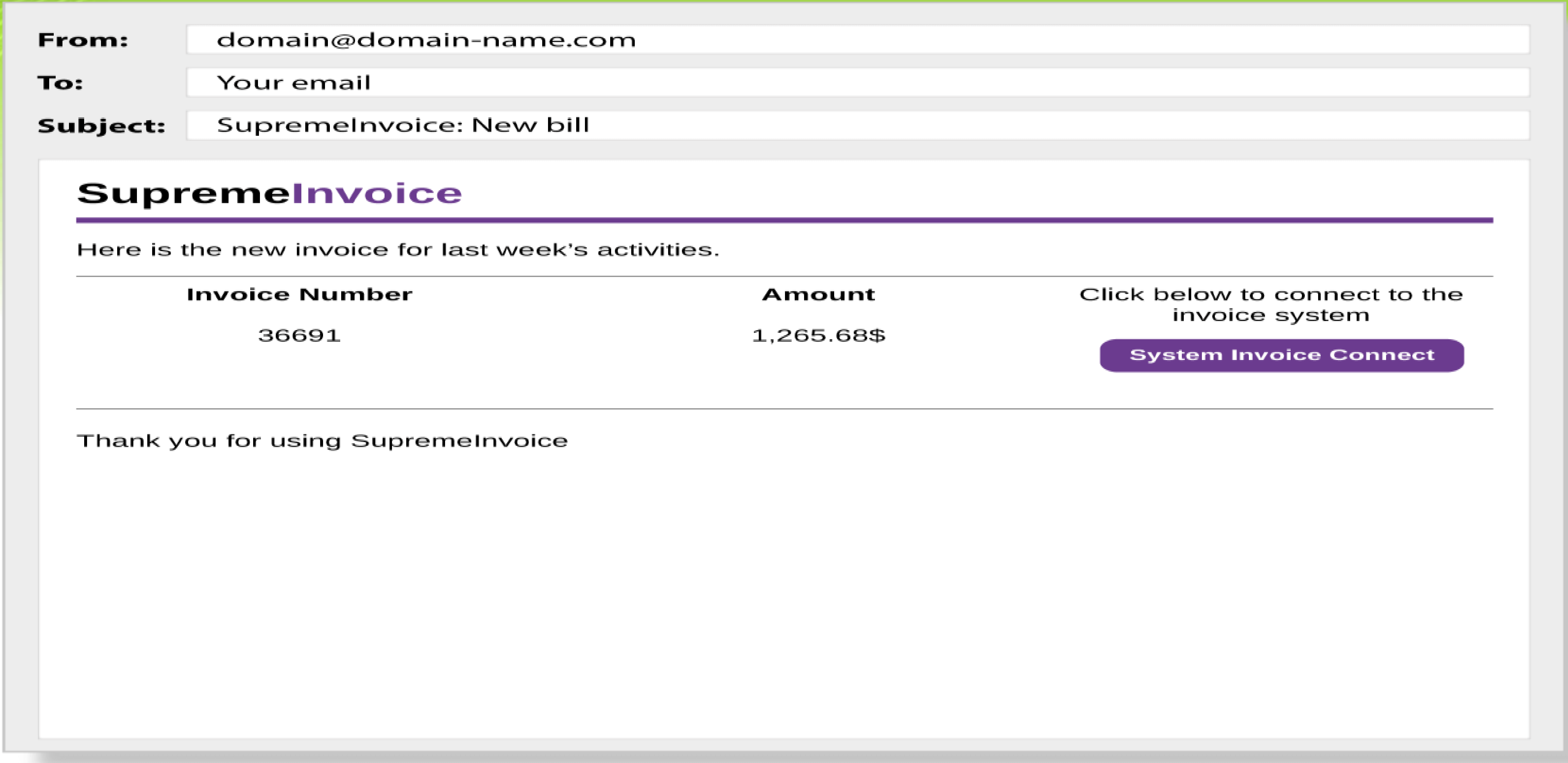
To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

Fake Google Docs Login



From: domain@domain-name.com

To: Your email

Subject: SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	System Invoice Connect

Thank you for using SupremeInvoice

Famous Phishing Incidents

Phishing is a major cybersecurity threat to organizations.

Proofpoint's 2022 report showed 83% of organizations experienced phishing attacks.

Verizon's 2021 report found 25% of all data breaches involve phishing.

These attacks are popular because they're easy and can be very profitable.

A convincing email and a targeted contact are often enough for success.

The Nordea Bank Incident (2007)

Swedish bank Nordea lost over 7 million kronor to phishing attacks.

Customers were tricked into installing the "haxdoor" Trojan disguised as anti-spam software.

The Trojan installed keyloggers and directed victims to a fake bank website, capturing login credentials.

Many victims lacked up-to-date antivirus protection.

Operation Phish Phry (2009)

One of the FBI's largest cybercrime busts, with $1.5 million stolen by cybercriminals in the U.S. and Egypt.

The phishing operation involved bank fraud.

FBI Director Robert Mueller highlighted the growing digital arms race and created the National Cyber Investigative Joint Task Force to combat such attacks.

RSA Incident (2011)

U.S. defense suppliers were breached when RSA fell for spear phishing.
An email disguised as recruitment plans targeted mid-level employees.
The message read: "I forward this file to you for review. Please open and view it."
One employee opening the email gave phishers backdoor access.
They bypassed SecurID two-factor authentication and stole company data.

Dyre Phishing Scam (2014)

Russian hacker group Dyre caused millions in losses through malware.
Phishers posed as tax consultants, tricking victims into downloading malicious files.
Victims included Sherwin-Williams, Miba, and RyanAir in the U.S., UK, and Australia.
If victims didn’t enter credentials, hackers called via Skype, pretending to be law enforcement.
Arrests were made in late 2015, but the attack led to the creation of TrickBot malware targeting financial institutions.

The Sony Pictures Leak (2014)

Sony suffered a massive data leak of over 100 terabytes, costing over $100 million.
Phishers posed as colleagues and tricked top-level employees into opening malicious attachments.
They used a fake Apple ID verification email in the attack.
By combining LinkedIn data with Apple ID logins, phishers found passwords that matched Sony's network.
This highlights the importance of using different passwords for various accounts.

Facebook & Google Scam

Facebook and Google lost $100 million in a phishing scam linked to Lithuania.
Despite an arrest, this incident shows even major tech companies can fall victim to phishing.

2018 World Cup Phishing

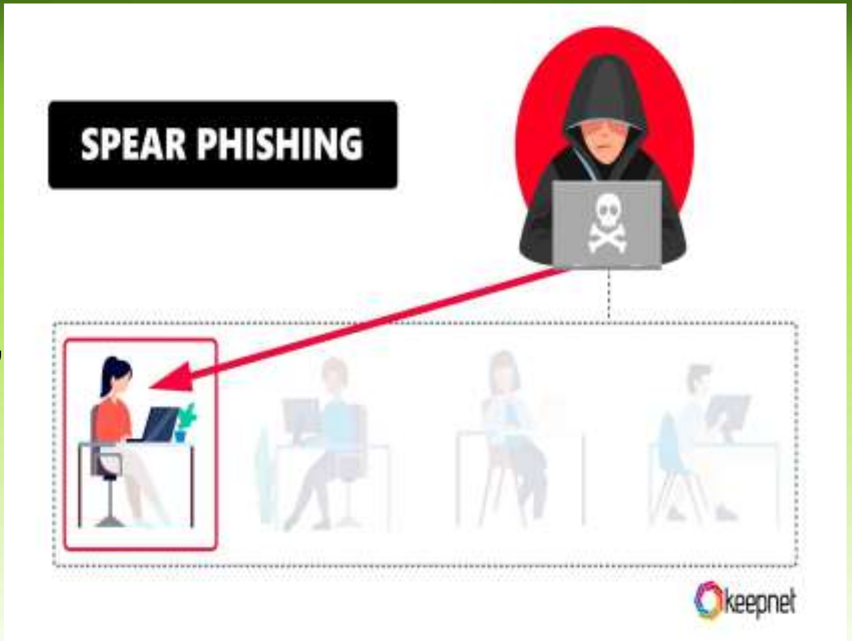
The FTC warned about phishing scams during the 2018 World Cup in Russia.
Scammers claimed victims had won tickets and asked for personal information.
Rental scams involved stolen emails from landlords, offering properties at low prices.
Once a victim accepted, their credit card information was stolen.

Types of Phishing

Spear Phishing

Spear phishing targets specific individuals within an organization to steal their login credentials.

Attackers gather information about the target, including their name, position, and contact details.



Example of Spear Phishing

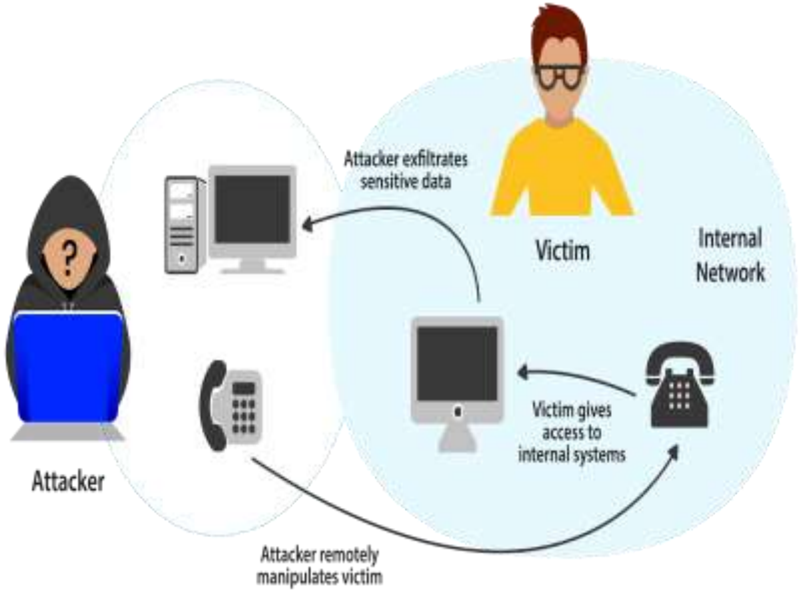
An attacker targeted an employee at NTL World (part of Virgin Media) claiming they needed to sign a new employee handbook.

This lured the victim into clicking a link to submit private information.

Vishing

Vishing (voice phishing) uses phone calls to steal information.

Attackers may impersonate trusted friends, relatives, or representatives.



Attacker exfiltrates sensitive data
Victim
Internal Network
Victim gives access to internal systems
Attacker
Attacker remotely manipulates victim

Example of Vishing

In 2019, a vishing campaign targeted UK parliament members and their staff.

This attack was part of a larger assault involving 21 million spam emails aimed at UK lawmakers.

Email Phishing

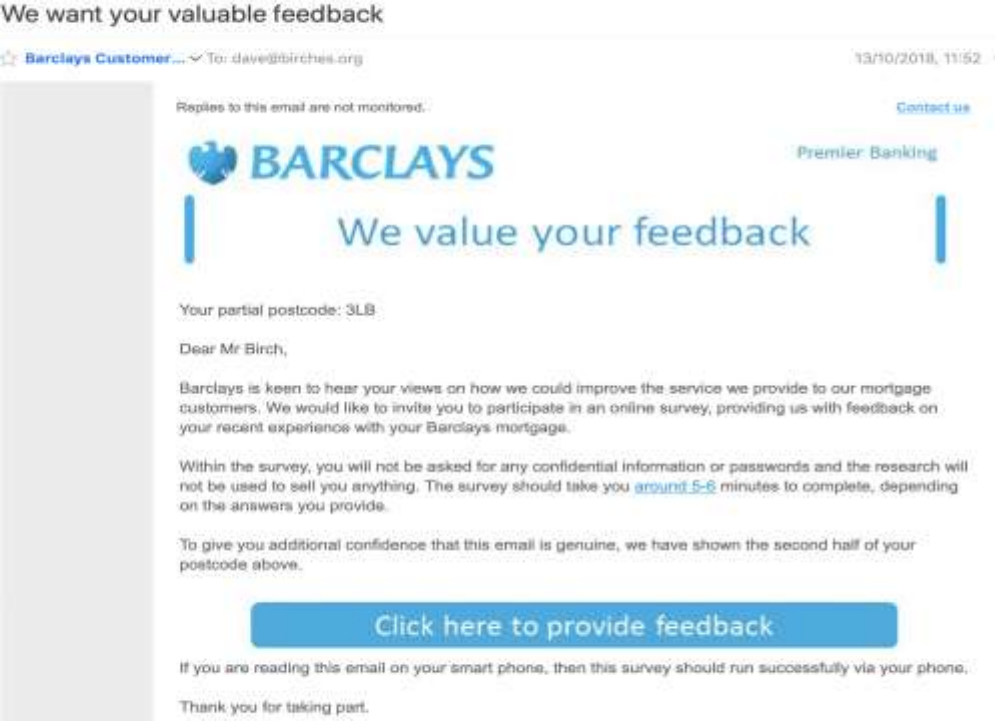
In email phishing, attackers send fake emails that appear legitimate.

The goal is to trick recipients into providing information or visiting a malicious site.

Example of Email Phishing

Hackers used LinkedIn to gather contact information from Sony employees.

They launched an email phishing campaign, resulting in over 100 terabytes of stolen data.



We want your valuable feedback

Barclays Customer... To: dave@birches.org 13/10/2018, 11:52

Replies to this email are not monitored. Contact us

BARCLAYS Premier Banking

We value your feedback

Your partial postcode: 3LB

Dear Mr Birch,

Barclays is keen to hear your views on how we could improve the service we provide to our mortgage customers. We would like to invite you to participate in an online survey, providing us with feedback on your recent experience with your Barclays mortgage.

Within the survey, you will not be asked for any confidential information or passwords and the research will not be used to sell you anything. The survey should take you around 5-6 minutes to complete, depending on the answers you provide.

To give you additional confidence that this email is genuine, we have shown the second half of your postcode above.

Click here to provide feedback

If you are reading this email on your smart phone, then this survey should run successfully via your phone.

Thank you for taking part.

HTTPS Phishing

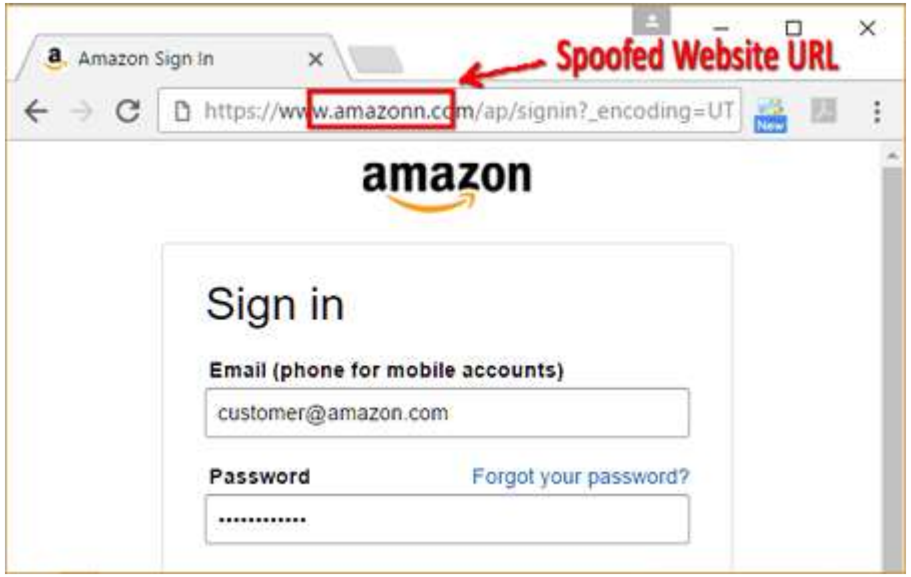
HTTPS phishing involves sending emails with links to fake websites.

These sites deceive victims into entering their private information.

Example of HTTPS Phishing

The hacker group Scarlet Widow searches for employee emails to target.

They send mostly empty emails, prompting users to click on a small link, leading them into the scam.



Pharming

In a pharming attack, malicious code is installed on the victim's computer.

This code redirects the victim to a fake website designed to steal login credentials.

Example of Pharming

In 2007, a complex pharming attack targeted at least 50 financial institutions worldwide.

Users were sent to fake websites and prompted to enter sensitive information.

Pharming Attack
Sends user to fake website instead of the real website the user intended to visit.
Web User
Hacker
Fake website

Pop-Up Phishing

Pop-up phishing uses alerts about computer security issues to trick users into clicking.

Victims may be directed to download malware or call a fake support center.

Example of Pop-Up Phishing

Users have received pop-ups claiming they qualify for AppleCare renewal, offering fake extended protection for Apple devices.

Evil Twin Phishing

In an evil twin attack, hackers create a fake Wi-Fi network that appears legitimate.

When users connect and enter sensitive information, the hacker captures their data.

Example of Evil Twin Phishing

The Russian military agency GRU was charged with executing evil twin attacks using fake access points.

These access points mimicked real networks but directed users to sites that stole credentials or installed malware.

Watering Hole Phishing

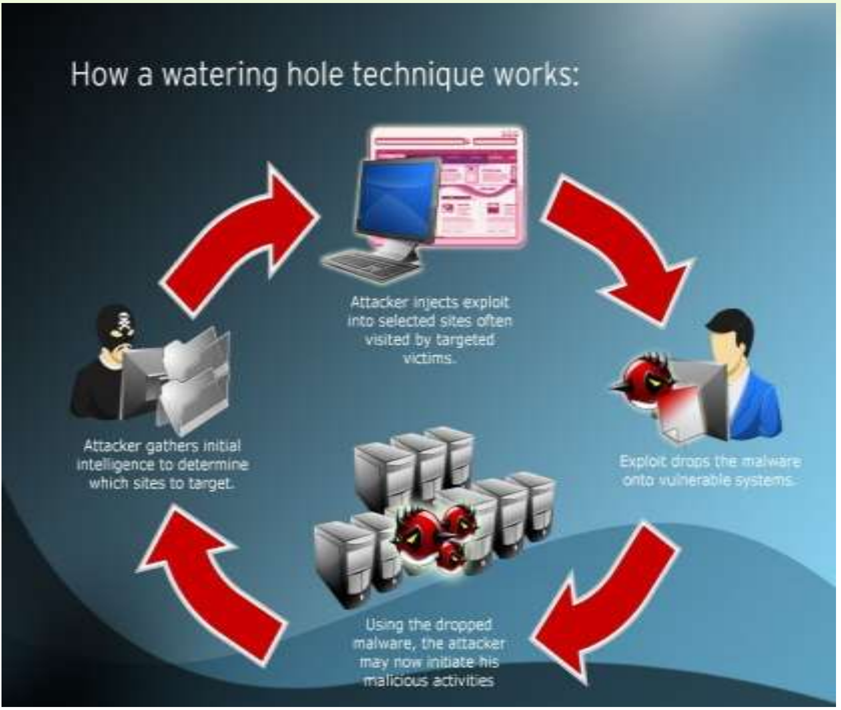
In a watering hole attack, hackers identify a website frequented by a specific group of users.

They infect this site to compromise users' computers and penetrate the network.

Example of Watering Hole Phishing

In 2012, the U.S. Council on Foreign Relations was targeted by a watering hole attack.

The assault aimed to exploit high-profile users and their login credentials, succeeding through a vulnerability in Internet Explorer.


How a watering hole technique works:
Attacker injects exploit into selected sites often visited by targeted victims.
Exploit drops the malware onto vulnerable systems.
Using the dropped malware, the attacker may now initiate his malicious activities
Attacker gathers initial intelligence to determine which sites to target.

Whaling

A whaling attack targets senior executives who have access to sensitive network areas.

Successful attacks can lead to valuable information being compromised.

Example of Whaling

The founder of Levitas, an Australian hedge fund, was targeted in a whaling attack.

They clicked a fraudulent Zoom link, resulting in malware installation and a loss of $800,000.

Clone Phishing

Clone phishing involves hackers creating an identical copy of a legitimate message the recipient has already received.

The hacker may include a note like "resending this" and insert a malicious lin

Example of Clone Phishing

In a recent attack, a hacker copied a previous email from a legitimate contact

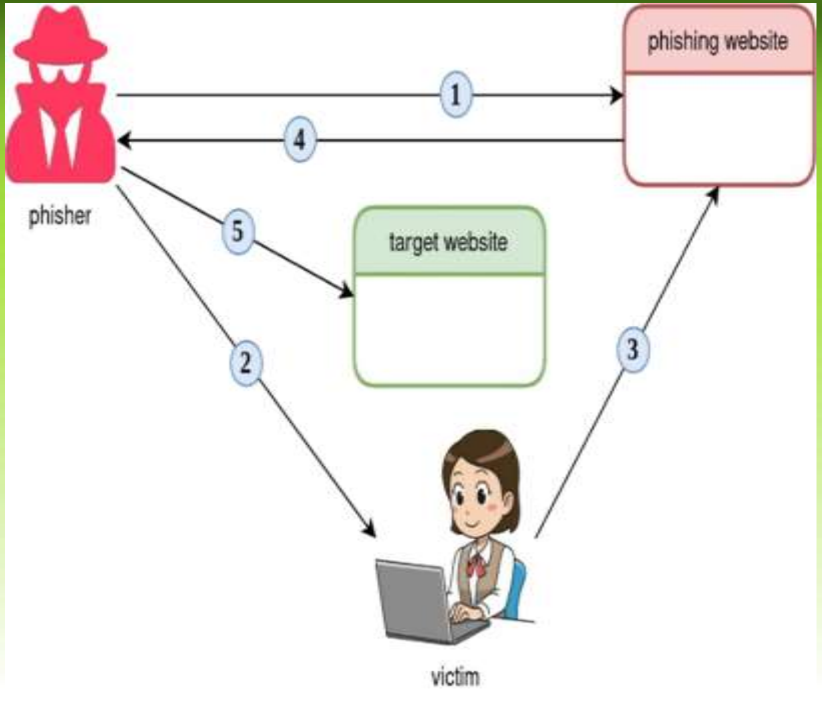
Pretending to be CEO Giles Garcia, the hacker referenced the earlier email and continued the conversation as if they were the real person.

Deceptive Phishing

Deceptive phishers use fraudulent techniques to pose as legitimate companies.
They inform targets of a supposed cyberattack, prompting them to click on malicious links that infect their computers.

Example of Deceptive Phishing

Victims received emails from support@apple.com with “Apple Support” in the sender information.
The message claimed the victim’s Apple ID was blocked and prompted them to validate their account by entering sensitive information.

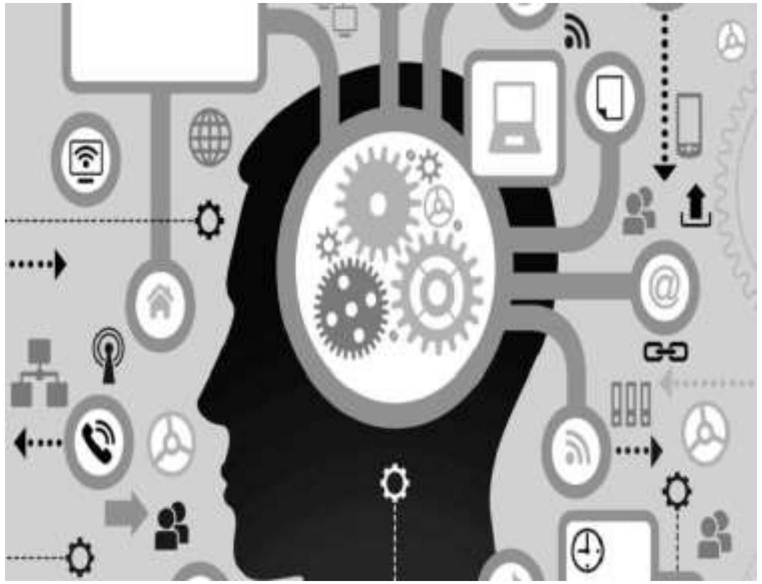


Social Engineering

Social engineering attacks manipulate individuals psychologically to reveal sensitive information.

Example of Social Engineering

A hacker pretended to be a Chase Bank representative, claiming action was needed on the target’s debit or ATM card.
The attacker pressured the victim by exploiting their fear of losing access to their funds.

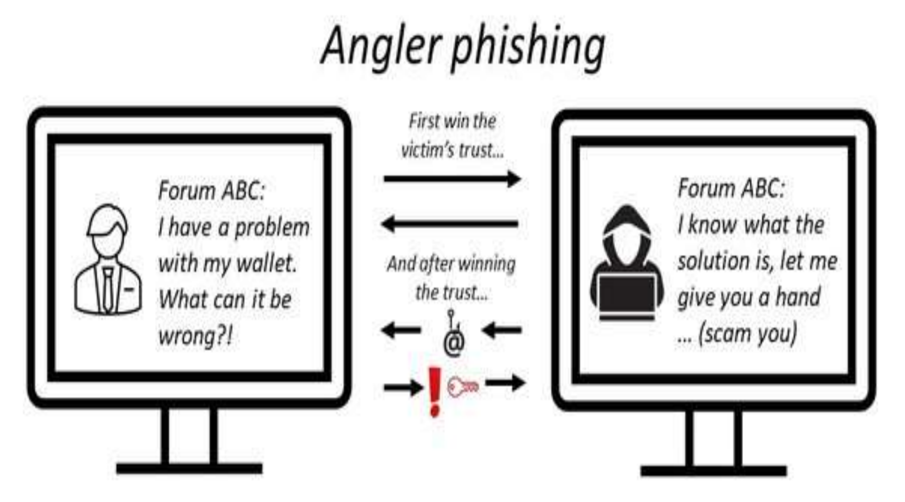


Angler Phishing

Angler phishing uses fake social media posts to trick people into providing login info or downloading malware.

Example of Angler Phishing

Hackers pretended to represent Domino's Pizza on Twitter, responding to customer concerns.
Once engaged, they used the situation to obtain personal information under the guise of offering refunds or rewards.


Angler phishing
Forum ABC:
I have a problem with my wallet. What can it be wrong?!
First win the victim's trust...
And after winning the trust...
Forum ABC:
I know what the solution is, let me give you a hand ... (scam you)

Smishing

Smishing is phishing conducted through text messages or SMS.

Example of Smishing

Hackers impersonated American Express and sent urgent text messages to victims.
The messages prompted victims to click a link, leading to a fake site to enter personal information.

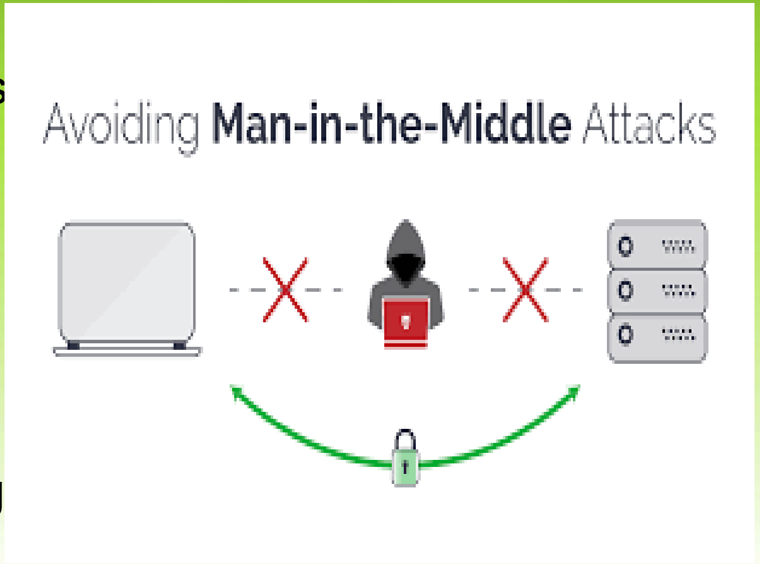
Smishing
(SMS-Phishing)
It's a type of Social Engineering
That targets mobile devices

Man-in-the-middle (MITM) attacks

With a man-in-the-middle attack the hacker gets in “the middle” of two parties and tries to steal information exchanged between them, such as account credentials.

Example of man-in-the-middle attack

In 2017, Equifax, the popular credit score company, was targeted by man-in-the-middle attacks that victimized users who used the Equifax app without using HTTPS, which is a secure way to browse the internet. As the users accessed their accounts, the hackers intercepted their transmissions, stealing their login credentials.

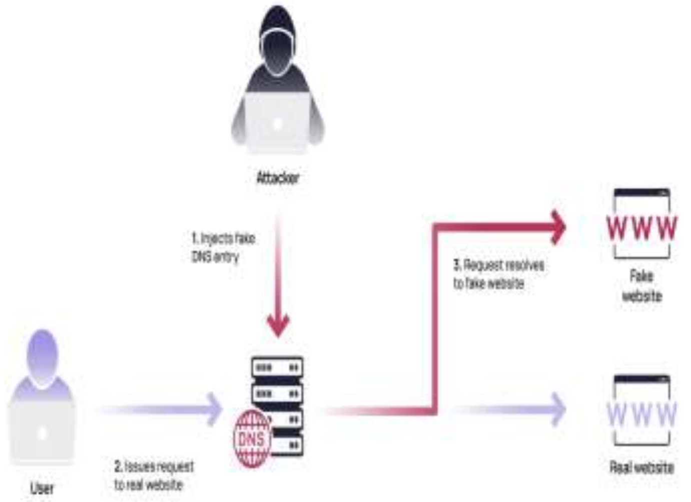


Website spoofing

With website spoofing, a hacker creates a fake website that looks legitimate. When you use the site to log in to an account, your info is collected by the attacker.

Example of website spoofing

Hackers made a fake Amazon website that looked nearly identical to the real Amazon.com but had a different Uniform Resource Locator (URL). All other details, including fonts and images, looked legitimate. Attackers were hoping that users would put in their username and password.


Attacker
1. Injects fake DNS entry
3. Request resolves to fake website
WWW
Fake website
DNS
User
2. Issues request to real website
WWW
Real website

Domain Spoofing

Domain spoofing (DNS spoofing) involves hackers imitating a company’s domai through fake websites or emails to steal sensitive information.
To prevent it, always double-check the source of links and emails.

Example of Domain Spoofing

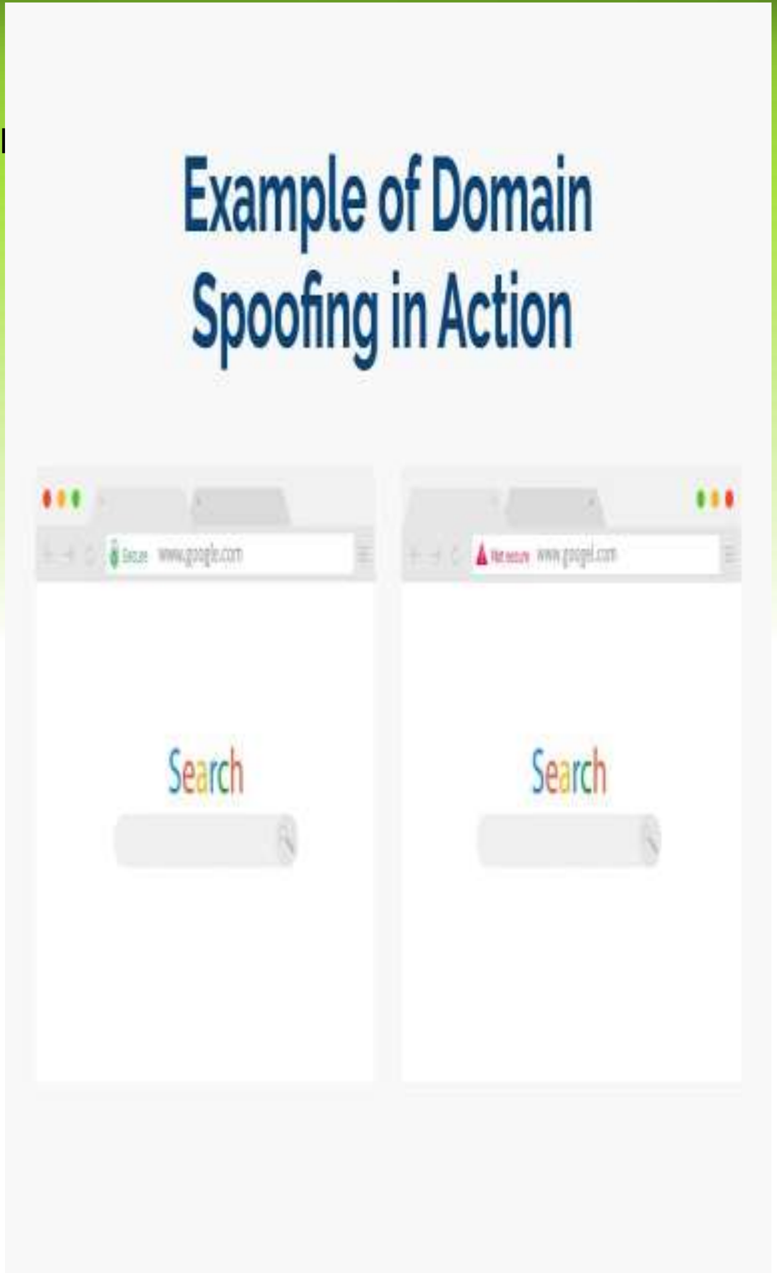
An attacker might create a fraudulent domain resembling LinkedIn.
When users enter information, it is sent directly to the hacker.

Image Phishing

Image phishing uses images with hidden malicious files to steal account info or infect computers.

Example of Image Phishing

Hackers used AdGholas to embed JavaScript malware in images.
Clicking the image downloaded malware, enabling phishing attacks to steal personal information.

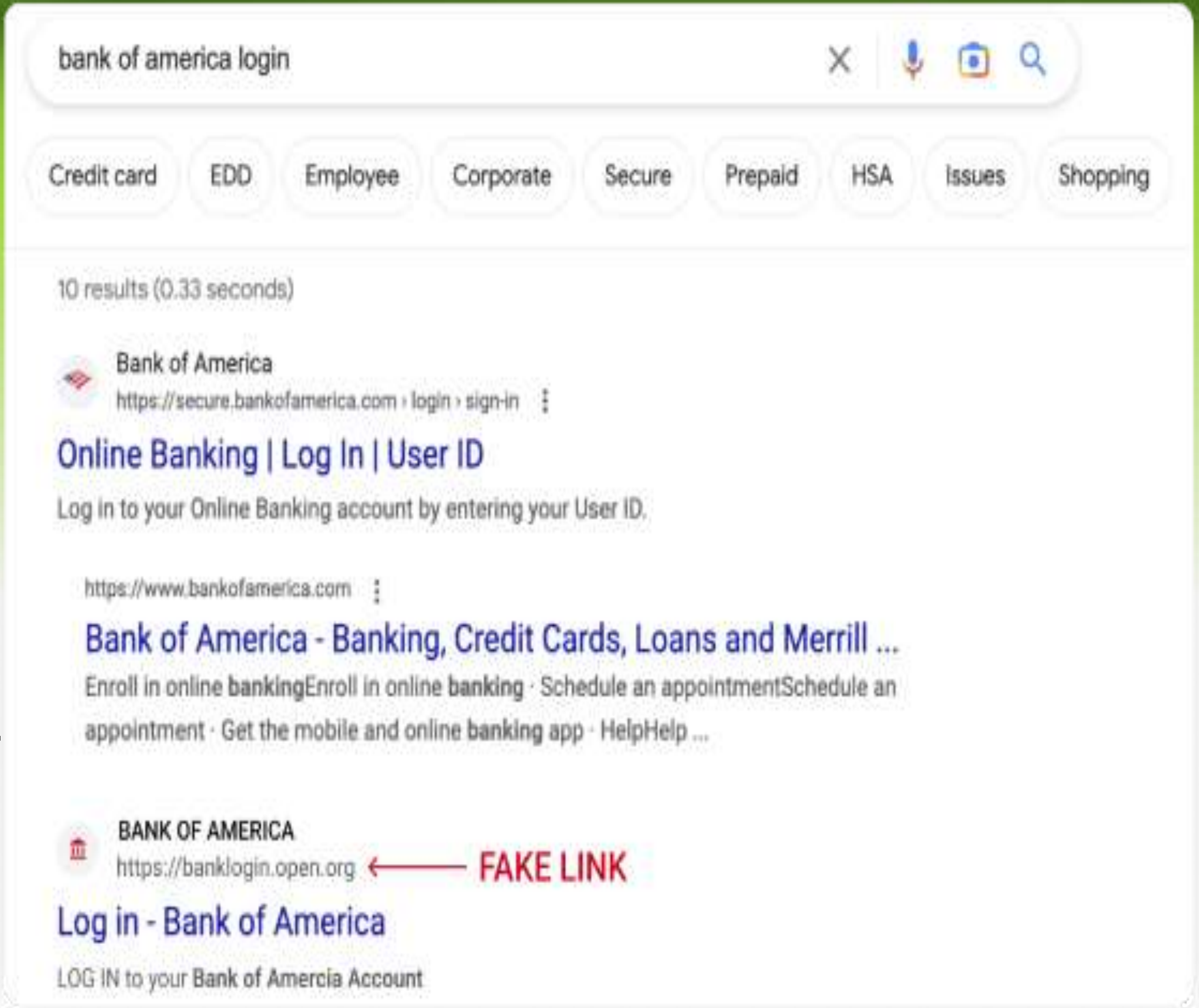

Example of Domain Spoofing in Action
Secure www.google.com
Not secure www.googel.com
Search
Search

Search Engine Phishing

Search engine phishing involves attackers creating fake products or websites that appear in search results.
When users click and attempt to purchase, they enter sensitive information, which goes to the hacker.

Example of Search Engine Phishing

In 2020, Google found 25 billion spam pages daily, including fake ads mimicking Booking.com. Users were prompted to enter login information after clicking, which was then sent to hackers.



bank of america login

10 results (0.33 seconds)

Bank of America
https://secure.bankofamerica.com › login › sign-in

Online Banking | Log In | User ID

Log in to your Online Banking account by entering your User ID.

https://www.bankofamerica.com

Bank of America - Banking, Credit Cards, Loans and Merrill ...

Enroll in online bankingEnroll in online banking · Schedule an appointmentSchedule an appointment · Get the mobile and online banking app · HelpHelp ...

BANK OF AMERICA
https://banklogin.open.org ⟵ FAKE LINK

Log in - Bank of America

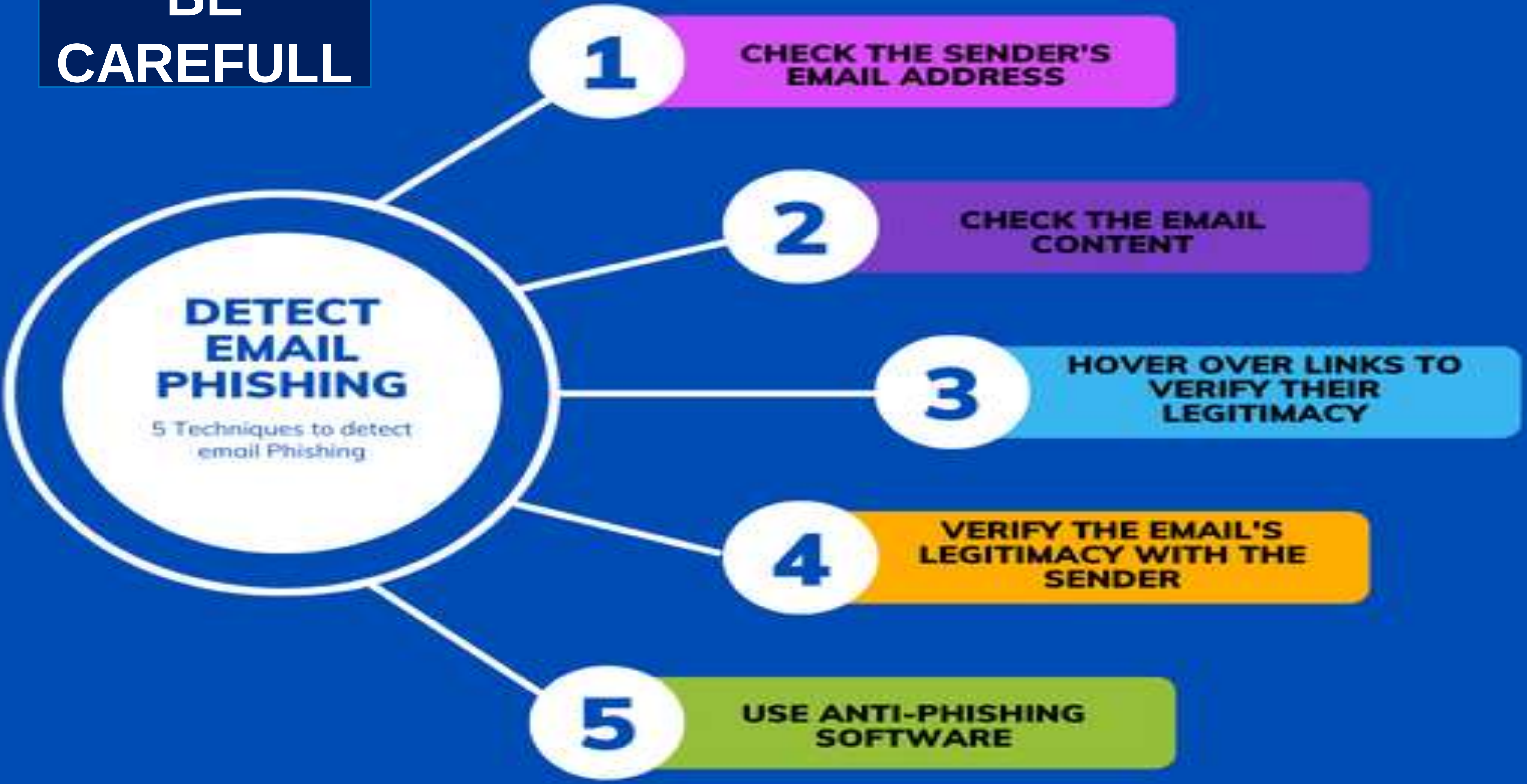
LOG IN to your Bank of Amercia Account

How to Spot Phishing Scams

Recognizing phishing attempts is essential for protecting your business and data. Here are key signs to look out for:

- **Urgent Action Demands:** Attackers create a sense of urgency to push hasty decisions before careful examination.
- **Poor Grammar & Spelling:** Phishing emails often contain grammar and spelling errors, unlike professional communication.
- **Unusual Greetings:** Formal or odd greetings that don’t match normal office communication are a red flag.
- **Inconsistent Links, Addresses & Domains:** Hover over links to verify them. Be wary of familiar names with strange domains.
- **Suspicious Attachments:** Unexpected attachments, even from known contacts, should be double-checked.
- **Too Good to Be True Offers:** Be cautious of rewards or incentives from unfamiliar senders.
- **Unexpected Requests:** Emails requesting personal info from managers or colleagues, especially urgent ones, could be phishing.
- **Requests for Sensitive Information:** Always verify emails asking for sensitive data and login pages to ensure authenticity.

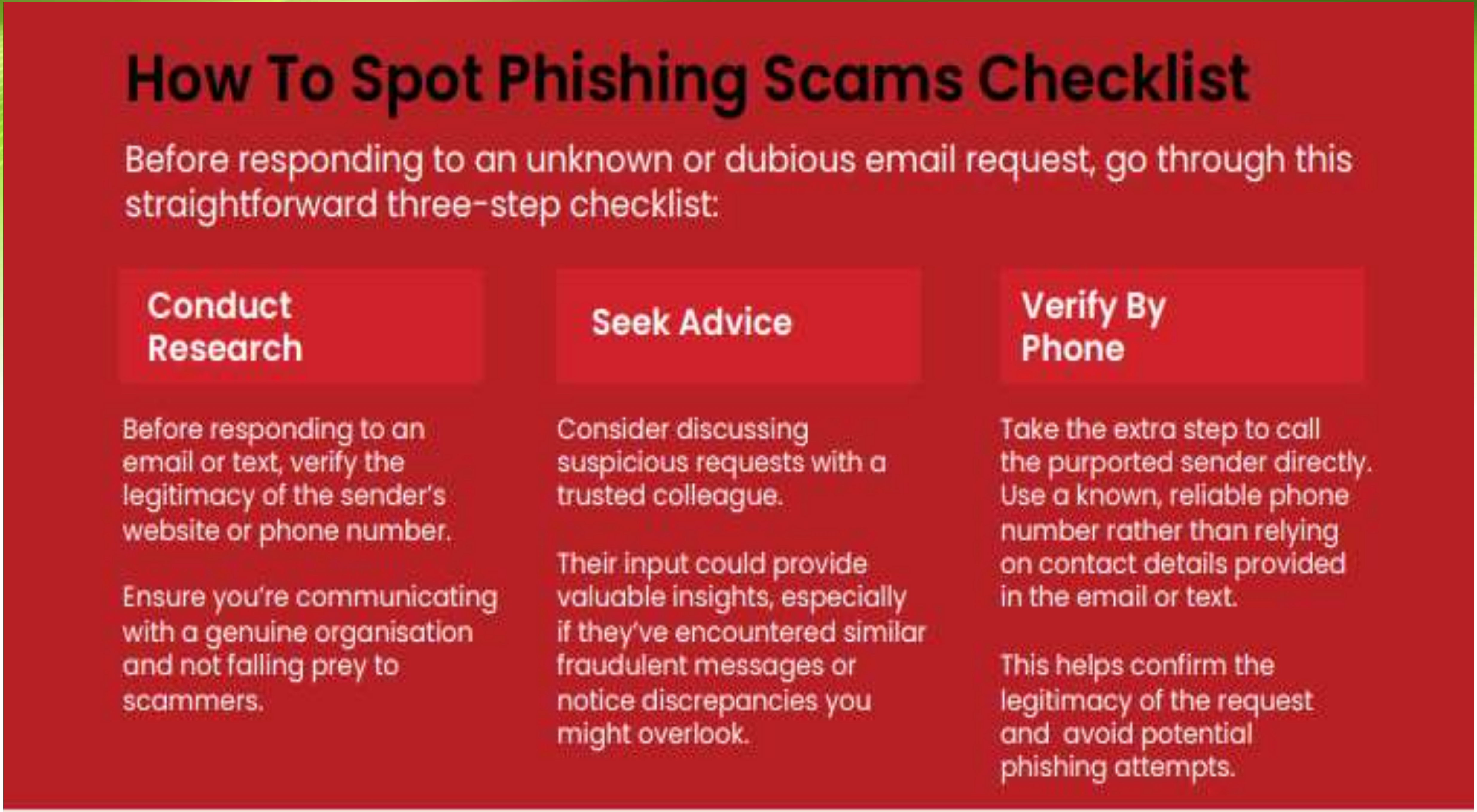
BE CAREFULL



DETECT EMAIL PHISHING

5 Techniques to detect email Phishing

1. CHECK THE SENDER'S EMAIL ADDRESS
2. CHECK THE EMAIL CONTENT
3. HOVER OVER LINKS TO VERIFY THEIR LEGITIMACY
4. VERIFY THE EMAIL'S LEGITIMACY WITH THE SENDER
5. USE ANTI-PHISHING SOFTWARE



How To Spot Phishing Scams Checklist

Before responding to an unknown or dubious email request, go through this straightforward three-step checklist:

Conduct Research

Before responding to an email or text, verify the legitimacy of the sender's website or phone number.

Ensure you're communicating with a genuine organisation and not falling prey to scammers.

Seek Advice

Consider discussing suspicious requests with a trusted colleague.

Their input could provide valuable insights, especially if they've encountered similar fraudulent messages or notice discrepancies you might overlook.

Verify By Phone

Take the extra step to call the purported sender directly. Use a known, reliable phone number rather than relying on contact details provided in the email or text.

This helps confirm the legitimacy of the request and avoid potential phishing attempts.

How to Recognize Advanced Phishing Attempts

- **Similar-Looking Email Addresses: C**heck for small inconsistencies, such as extra characters, domain mismatches, or foreign-language URLs that resemble legitimate addresses.

- **Compromised Legitimate Accounts:** Be cautious of phishing emails sent from within an organization's trusted network, as attackers may compromise real accounts.

- **Requests for Sensitive Info or Urgent Action:** Advanced phishing often uses authority, urgency, or fear (e.g., financial loss or legal issues) to pressure users into quick action.
  Authentic-Looking Emails: Phishers can replicate official emails with logos, formatting, and corporate language. If anything feels off, proceed with caution.

- **Multi-Vector Attacks:** Phishing campaigns may use multiple communication channels (emails, texts, calls) at once. Unexpected multiple messages are a red flag.

Strategies for Preventing a Phishing Attack

- **Phishing Awareness Training:** Educate employees on recognizing phishing attempts and what steps to take. Research shows 80% of organizations report reduced susceptibility after training.
- **Simulated Phishing Attacks:** Use simulations to reinforce training and improve learning retention. This helps employees apply their knowledge to real-world scenarios, doubling vigilance.
- **Endpoint Protection Tools:** Deploy tools with anti-phishing features, like blacklists of known phishing sites, email security tools, and device-wide monitoring.
- **Verification Policies:** Implement policies requiring multiple approvals for payments, and ensure payments are processed only through approved, secure channels. Be cautious of payment methods like gift cards or cryptocurrencies.
- **Zero Trust Model:** Limit employees’ access to only the systems and data necessary for their job, reducing the potential damage of a phishing attack.
- **Next-Generation Identity Technologies:** Adopt passwordless authentication methods like passkeys, which are phishing-resistant and provide continuous threat protection.

Signs of a Phishing Phone Call

- "You've been specially selected for this offer."
- "You'll get a free bonus if you buy our product."
- "You've won one of five valuable prizes."
- "You've won big money in a foreign lottery."
- "This investment is low-risk and gives a higher return than anywhere else."
- "You have to decide right away."
- "You trust me, right?"
- "No need to check our company with anyone."
- "We'll just charge the shipping and handling to your credit card."

Tips to Protect Yourself from Phishing Phone Calls

- ❖ Avoid buying from unfamiliar companies; legitimate businesses will provide information willingly.
- ❖ Check unfamiliar companies with local consumer protection agencies or watchdog groups like the Better Business Bureau.
- ❖ Always get and verify the salesperson’s name, business identity, phone number, and address before doing business.
- ❖ Never pay for a "free prize"—paying for taxes on such prizes is illegal.
- ❖ Do not share personal information (credit card details, social security numbers) with unknown companies.
- ❖ Be cautious of calls offering to help recover losses for a fee paid in advance.

Tips to Protect Yourself from Phishing Emails

- I.T. will never ask for passwords via email. Be cautious of any email requesting your password or other private details.
- Avoid opening unexpected attachments or downloading files, even from known contacts, as they may contain malware. Confirm with the sender if unsure.
- Never enter personal information in a pop-up window. It’s a common phishing tactic.
- Hover over links to verify the destination before clicking.
- Ensure websites use 'https://' and display a lock icon before entering sensitive information.
- Watch for spelling or grammar errors, as legitimate companies usually avoid such mistakes in mass emails.

What to Do When You Think You Received a Phishing Email

- Do not click on any links or download attachments.
- Forward the email to abuse@valdosta.edu for Information Security to review.
- If the email has an attachment from a known sender, but you weren't expecting it, call them to confirm its legitimacy.