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
- Q&A Session

Presented by

- **Muhammad Ahmad** (Vulnerability assessment EXPERT)
- BSIT (UNIVERSITY OF OKARA)
- CEH (UNIVERSITY OF LAHORE)

Experience
Teaching (2019-2022)
Front Desk Operator (2022-Continue)

Contact # +923406267764
EMAIL # wwwahmadchaudhary90@gmail.com
LinkedIn # www.linkedin.com/in/muhammad-ahmad-36a863320

Phishing

Phishing is a type of fraudulent activity, committed by a person or a group of persons, on internet users, with the intent to trick them into revealing confidential or personal information.

What is a phishing attack?

Phishing attacks involved tricking a victim into taking some action that benefits the attacker. These attacks range from simple to complex, and can be spotted with the right awareness.

Usually, the attacker sends a fraudulent link or email, to snatches personal data from the user's computer or mobile. There are various techniques through which people get tricked into sharing sensitive information – text messages, spam emails and social media are common techniques.

Definitions

- A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
  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 Does a Phishing Attack Happen?

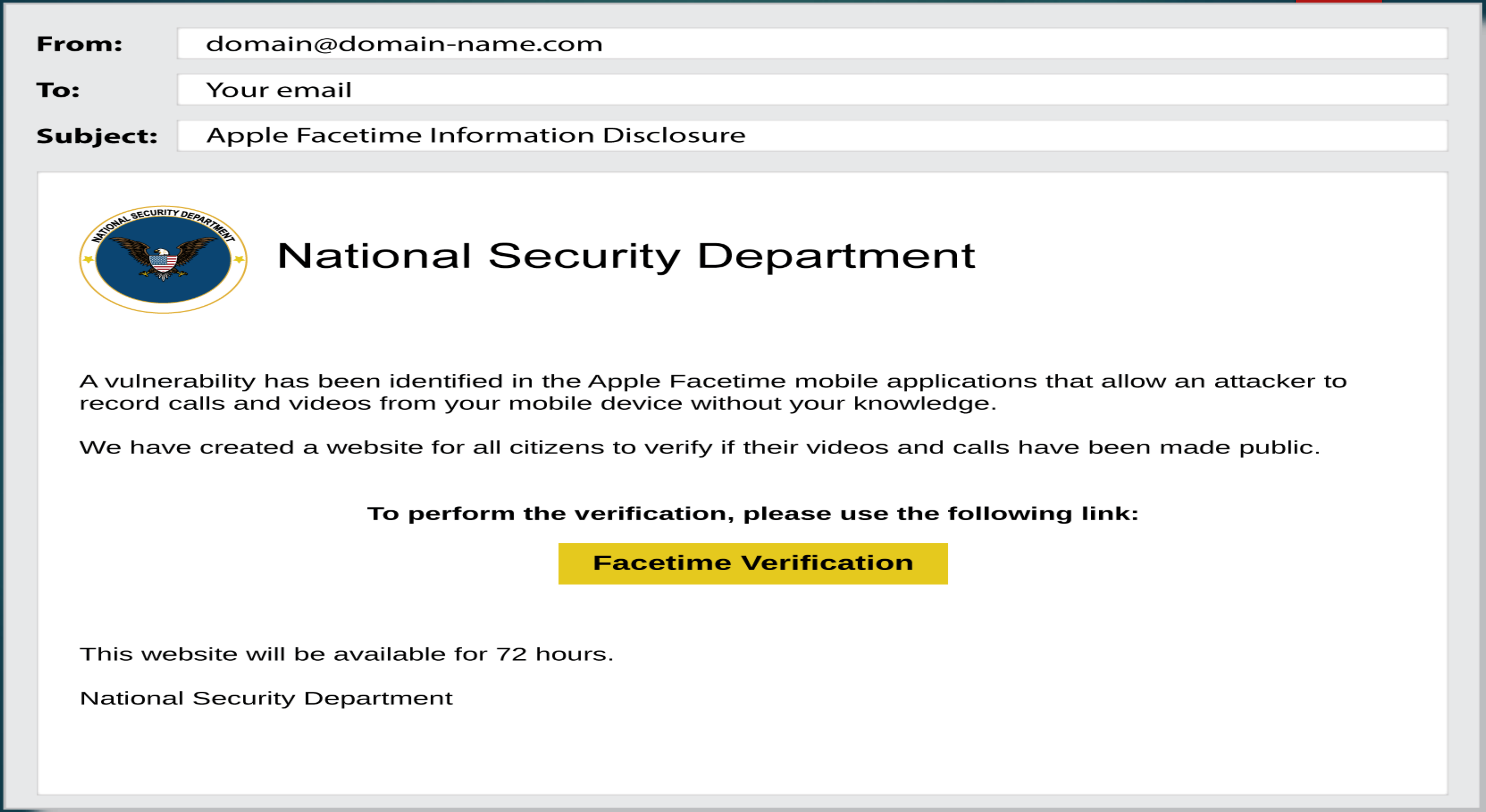
Phishing happens when a victim acts on a fraudulent email that demands urgent action. Examples of requested actions in a phishing email include:

- Clicking an attachment
- Enabling macros in a Word document
- Updating a password
- Responding to a social media friend or contact request
- Connecting to a new Wi-Fi hotspot

Every year, cybercriminals become savvier with their phishing tactics, improve their techniques, and try new methods to deceive and steal from unsuspecting people. Now, you can expect phishing through voicemails, texts, and emails.

Real-World Examples of Phishing Email Attacks

Social engineering tactics are one common thread that runs through all types of phishing emails, including the examples below. Like most phishing attacks, social engineering preys on the natural human tendency to trust people and companies. This leads many users to fail to carefully review phishing email details and automatically trust the sender’s request. Email phishing victims believe they’re helping their organizations by transferring funds, updating login details, or providing access to proprietary data.



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.

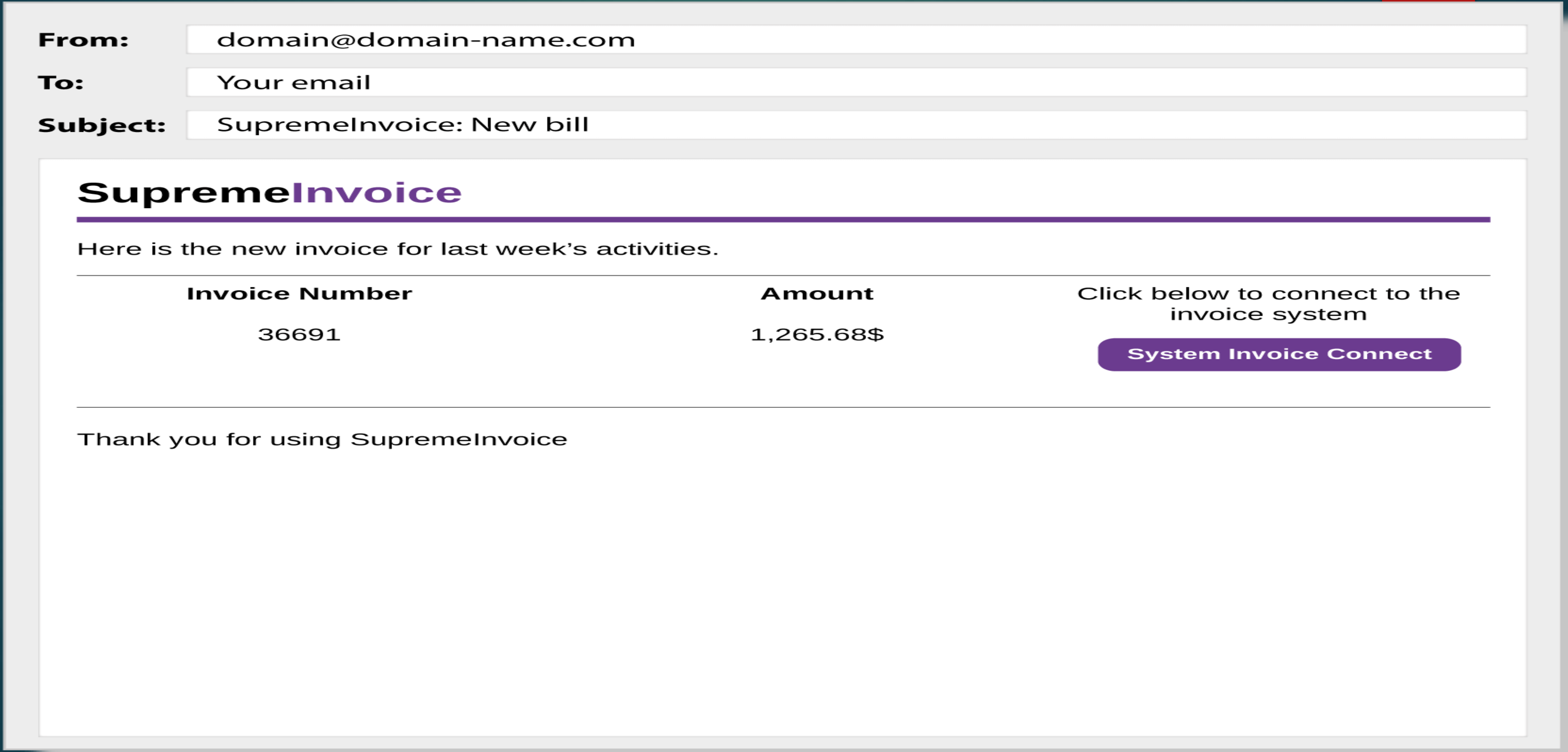
We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

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 from History

- Phishing is one of the greatest cyber security threats that organizations face. According to Proofpoint’s 2022 State of the Phish Report, 83% of organizations fell victim to a phishing attack last year.
- Meanwhile, Verizon’s 2021 Data Breach Investigations Report found that 25% of all data breaches involve phishing.
- Such attacks are increasingly popular because they’re easy to conduct and can potentially net the crooks a huge payout. All that’s required is a well-crafted email, the contact details of someone in your organization and the very high likelihood that someone will take the bait.

The Nordea Bank Incident

- In 2007, Swedish bank Nordea lost over 7 million kronor when phishers managed to send fraudulent emails out to bank customers, luring them to install the "haxdoor" Trojan disguised as anti-spam software.
- Dubbed the "biggest ever online bank heist" by digital security company McAfee, Nordea customers were hit with phishing emails containing Trojan viruses that installed a keylogger into the victims' computers and directed them to a fake bank website where hackers intercepted login credentials.
- While the exact blame can't be reliably placed, it is worth noting that most customers failed to have a running antivirus installed on their machines.

Operation Phish Phry

- 2009 saw one of the FBI's biggest cybersecurity busts ever after $1.5 million was stolen via bank frauds by various cyber thieves located in the United States and Egypt.
- Former Director Robert Mueller noted that phishing attempts were a new part of the digital arms race, with cyber criminals always working to stay ahead of law enforcement by taking advantage of new developments in technology. He established the National Cyber Investigative Joint Task Force specifically designed for these kinds of attacks.

RSA

In 2011, the United States' defense suppliers were breached when security firm RSA fell victim to spear phishing due to an Adobe Flash vulnerability.

Disguised as recruitment plans for that year, the email targeted mid-level employees with just one line of text: "I forward this file to you for review. Please open and view it.". Only one employee had to open the email for phishers to gain backdoor access on the victim's desktop. The phishers then managed to bypass the company's SecurID two-factor authentication to steal company data.

Dyre Phishing Scam

In late 2014, malware produced by Russian hacker group Dyre resulted in the loss of millions of dollars. The phishers posed as tax consultants and convinced thousands of victims to download malicious executable files.

Dyre's long list of victims included paint and materials company Sherwin-Williams, engine parts manufacturer Miba, airliners RyanAir, and several other companies throughout the U.S., the UK, and Australia.

When the victim failed to enter their credentials into the fake phishing site, the hackers called the victim through Skype pretending to be law enforcement officers and bank employees to encourage the transfer. While the final arrests were made in late 2015, the legacy of the cyberattack lives on. A new phishing malware named TrickBot was created shortly after, using the same elements from Dyre to target similar financial institutions.

The Sony Pictures Leak

2014 also saw a huge data leak from Sony. Over 100 Terabytes containing confidential company activities were breached, resulting in well over $100 million lost. The phishers pretended to be colleagues of the top-level employees who opened the malicious attachments in the phishing emails. Specifically, a fake Apple ID verification email was used in the attack. Through a combination of LinkedIn data and Apple ID logins, the phishers managed to find passwords that matched the ones used for the Sony network - a great example of why using different passwords for different online accounts is so important.

Facebook & Google

This is a huge one. Two of the world's largest tech giants, Facebook and Google, lost $100 million in this single email scam from Lithuania. While an arrest was made, the story shows that even the most advanced tech entities are susceptible to phishing attacks.

2018 World Cup

The Federal Trade Commission released this statement regarding phishing attempts during the 2018 World Cup in Russia. The scam claimed the victim won tickets to the World Cup through a lottery and prompted them to enter their personal information to claim the prize.

At the same time, a handful of rental scams were reported as well. Cybercriminals stole the email addresses of genuine landlords in Russia and offered ridiculously low prices for their properties during the sporting event. Once a "lucky buyer" accepted the offer, his or her credit card information was stolen.

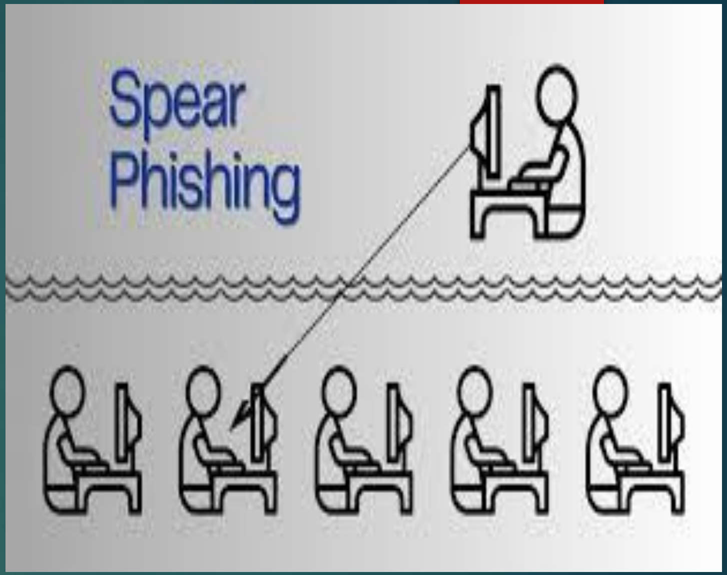
Types of Phishing

Spear phishing

Spear phishing involves targeting a specific individual in an organization to try to steal their login credentials. The attacker often first gathers information about the person before starting the attack, such as their name, position, and contact details.

Example of spear phishing

An attacker tried to target an employee of NTL World, which is a part of the Virgin Media company, using spear phishing. The attacker claimed that the victim needed to sign a new employee handbook. This was designed to lure them into clicking a link where they would have been asked to submit private information.

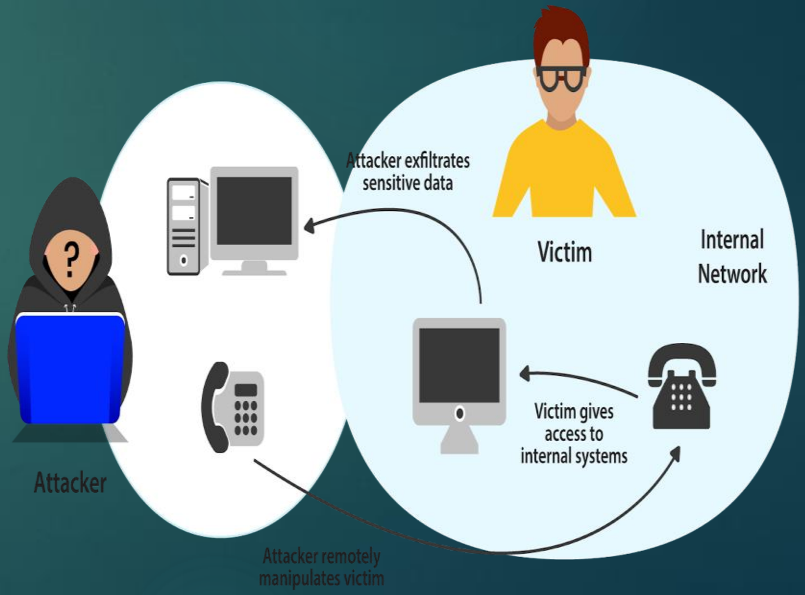


Vishing

Vishing, which is short for "voice phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.

Example of vishing

In 2019, there was a vishing campaign that targeted members of the UK's parliament and their staffers. The attack was part of an assault that involved at least 21 million spam emails targeting UK lawmakers.

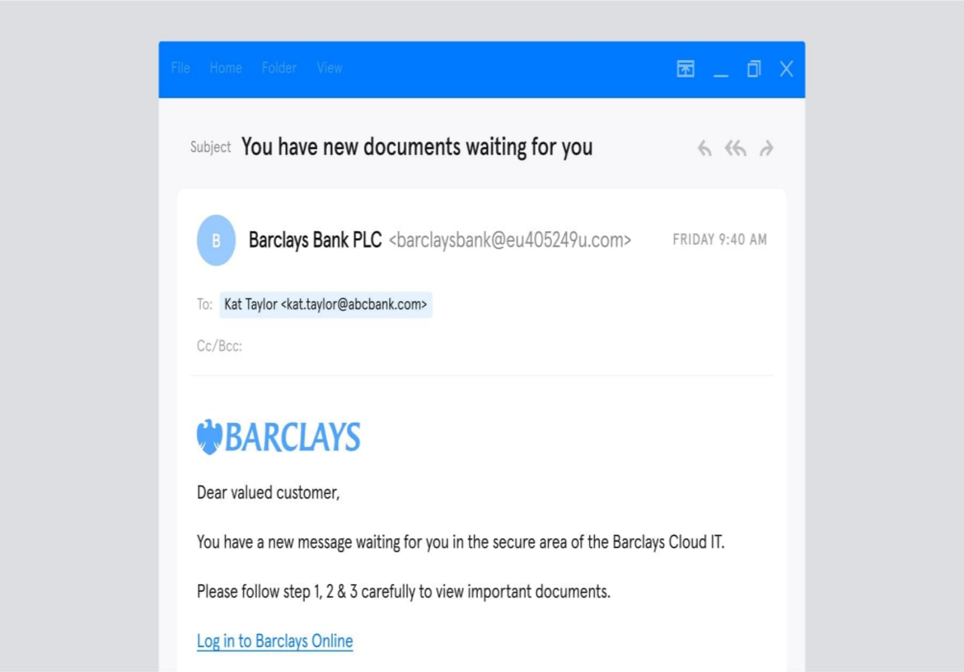

Attacker exfiltrates sensitive data
Victim
Internal Network
Attacker
Victim gives access to internal systems
Attacker remotely manipulates victim

Email phishing

In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.

Example of email phishing

Hackers used LinkedIn to grab contact information from employees at Sony and targeted them with an email phishing campaign. They got away with over 100 terabytes of data.



Subject You have new documents waiting for you

Barclays Bank PLC <barclaysbank@eu405249u.com> FRIDAY 9:40 AM

To: Kat Taylor <kat.taylor@abcbank.com>

Cc/Bcc:

Dear valued customer,

You have a new message waiting for you in the secure area of the Barclays Cloud IT.

Please follow step 1, 2 & 3 carefully to view important documents.

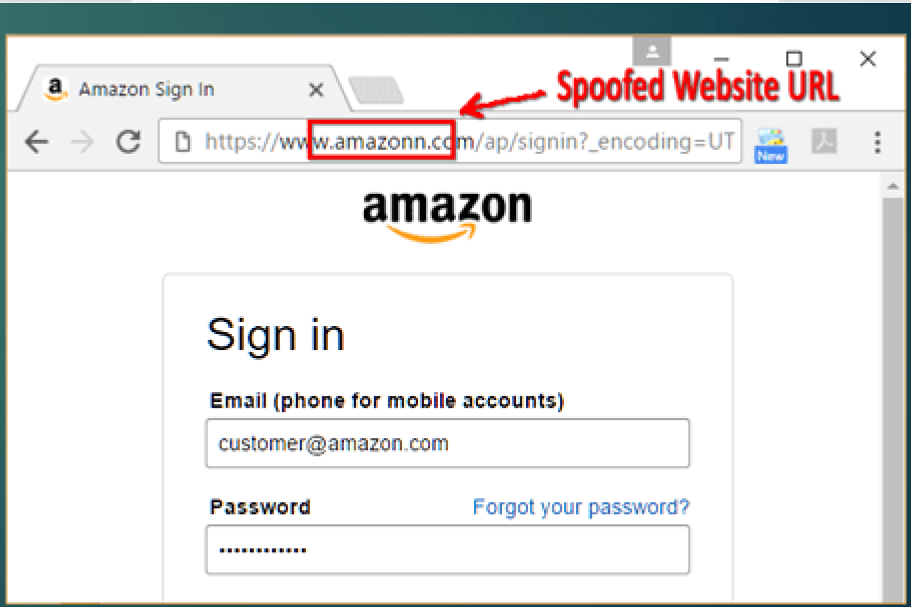
Log in to Barclays Online

HTTPS phishing

An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.

Example of HTTPS phishing

Hacker group Scarlet Widow searches for the employee emails of companies and then targets them with HTTPS phishing. When the user gets a mostly empty email, they click on the little link that is there, taking the first step into Scarlet Widow's web.



https://www.amazonn.com/ap/signin?_encoding=UT

Sign in

Email (phone for mobile accounts)

customer@amazon.com

Password Forgot your password?

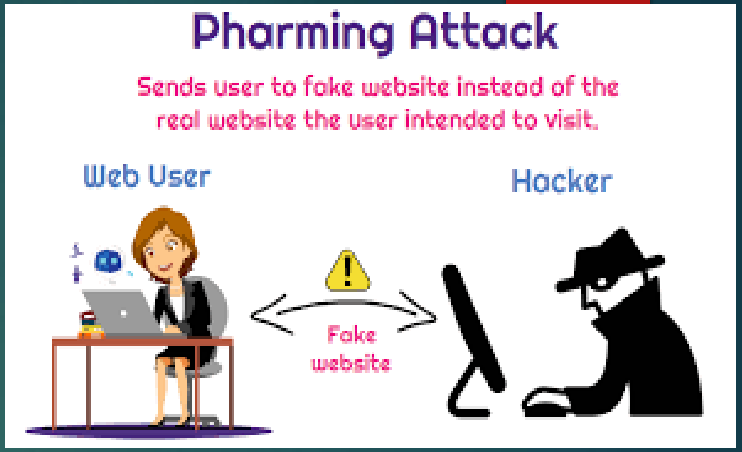
·············

Pharming

In a pharming attack, the victim gets malicious code installed on their computer. This code then sends the victim to a fake website designed to gather their login credentials.

Example of pharming

In 2007, a complex pharming attack went after at least 50 financial institutions across the world. Users were directed to false websites and instructed to enter sensitive information.

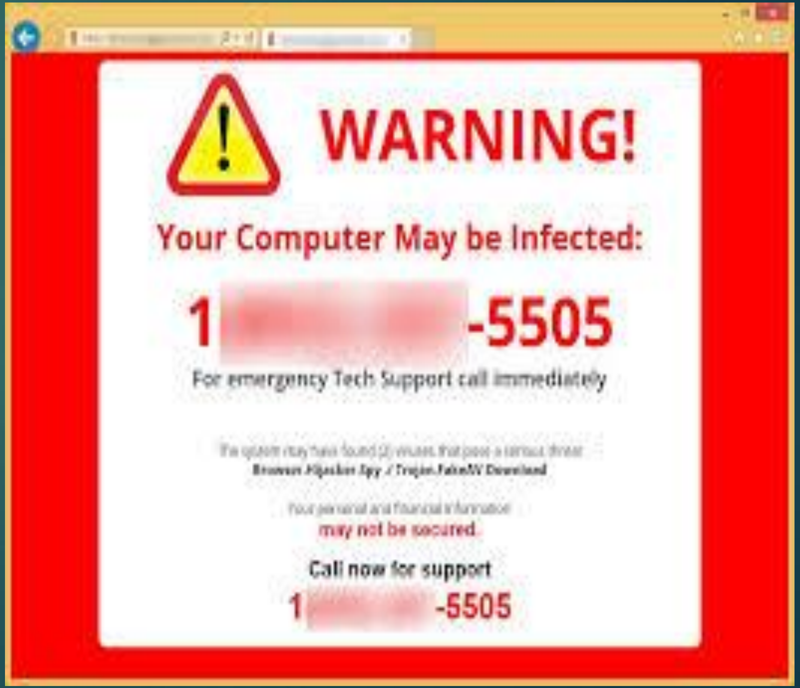

Pharming Attack
Sends user to fake website instead of the real website the user intended to visit.
Web User
Hacker
Fake website

Pop-up phishing

Pop-up phishing often uses a pop-up about a problem with your computer's security or some other issue to trick you into clicking. You are then directed to download a file, which ends up being malware, or to call what is supposed to be a support center.

Example of pop-up phishing

Users have sometimes received pop-ups saying they can qualify for AppleCare renewal which would supposedly avail them of extended protection for their Apple devices. However, the offer is fake.



WARNING!

Your Computer May be Infected:

1[redacted]-5505

For emergency Tech Support call immediately

The system may have found (2) viruses that pose a serious threat:
Browser Hijacker Spy / Trojan.FakeAV Download

Your personal and financial information
may not be secured.

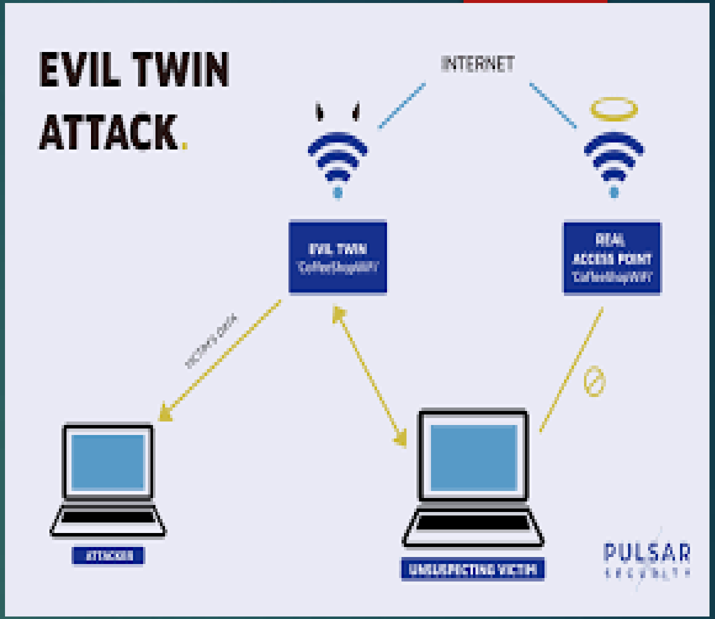
Call now for support
1[redacted]-5505

Evil twin phishing

In an evil twin attack, the hacker sets up a false Wi-Fi network that looks real. If someone logs in to it and enters sensitive details, the hacker captures their info.

Example of evil twin phishing

A Russian military agency called GRU was recently charged with executing evil twin attacks using fake access points. The access points were made to look like they provided connections to real networks when in reality they led users to sites that stole their credentials or downloaded malware onto their computers.

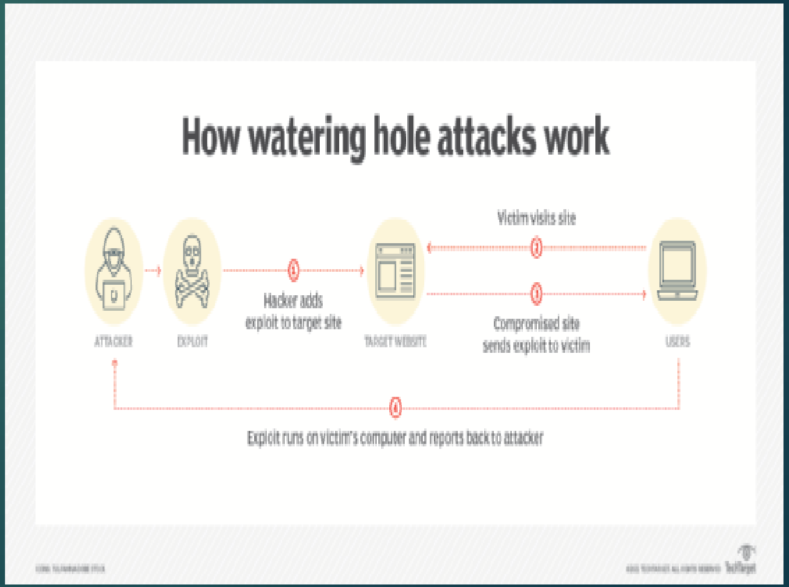


Watering hole phishing

In a watering hole phishing attack, a hacker figures out a site a group of users tends to visit. They then use it to infect the users' computers in an attempt to 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 take advantage of the high-profile users that were frequenting the site, as well as the login credentials they could provide. The attack achieved some success, particularly using a vulnerability within Internet Explorer.


How watering hole attacks work
ATTACKER
EXPLOIT
1
Hacker adds exploit to target site
TARGET WEBSITE
Victim visits site
2
3
Compromised site sends exploit to victim
USERS
4
Explcit runs on victim's computer and reports back to attacker
TechTarget

Whaling

A whaling attack is a phishing attack that targets a senior executive. These individuals often have deep access to sensitive areas of the network, so a successful attack can result in access to valuable info.

Example of whaling

A founder of Levitas, an Australian hedge fund was the target of a whaling attack that led the individual to a fake connection using a fraudulent Zoom link. After following the link, they had malware installed on their system, and the company lost $800.000.

Clone phishing

A clone phishing attack involves a hacker making an identical copy of a message the recipient already received. They may include something like “resending this” and put a malicious link in the email.

Example of clone phishing

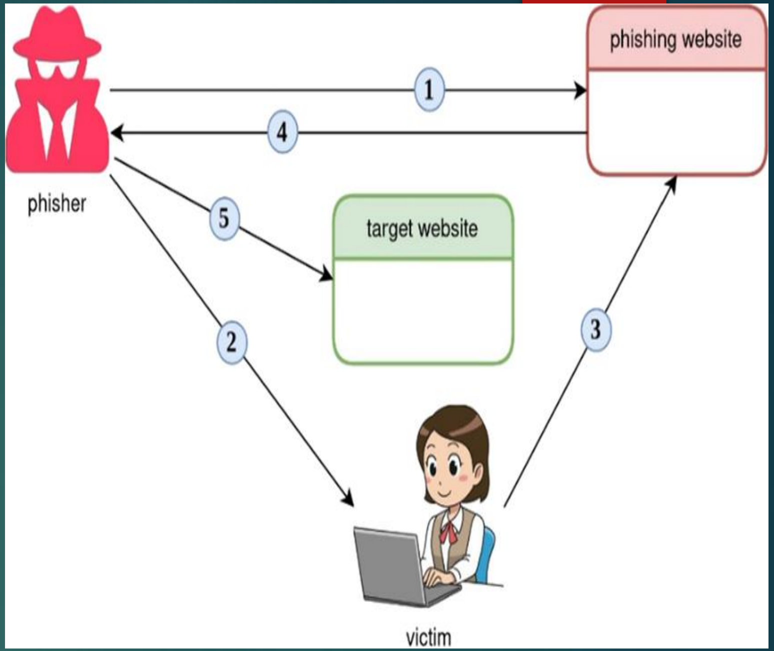
In a recent attack, a hacker copied the information from a previous email and used the same name as a legitimate contact that had messaged the victim about a deal. The hacker pretended to be a CEO named Giles Garcia and referenced the email Mr. Garcia had previously sent. The hacker then proceeded to pretend to carry on the previous conversation with the target, as if they really were Giles Garcia.

Deceptive phishing

Deceptive phishers use deceptive technology to pretend they are with a real company to inform the targets they are already experiencing a cyberattack. The users then click on a malicious link, infecting their computer.

Example of deceptive phishing

Users were sent emails that came from the address support@apple.com and had “Apple Support” in the sender information. The message claimed that the victim’s Apple ID had been blocked. They were then prompted to validate their accounts by entering information the hacker would use to crack it.

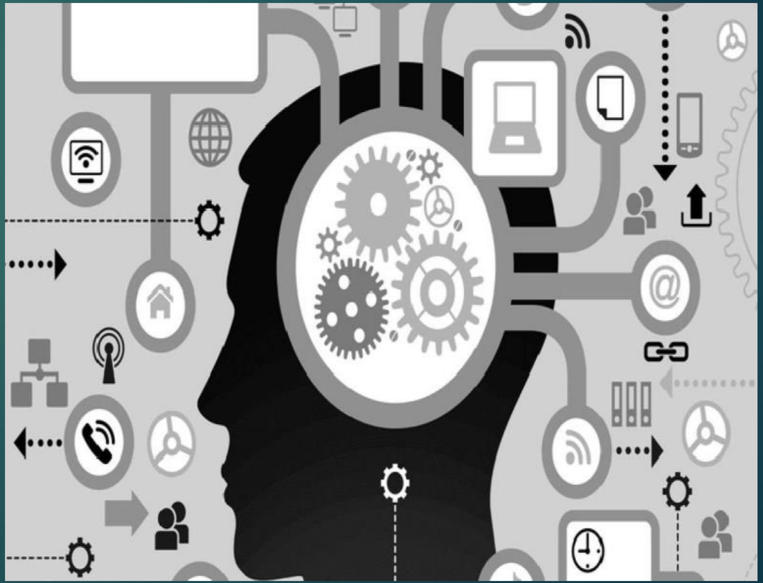


Social engineering

Social engineering attacks pressure someone into revealing sensitive information by manipulating them psychologically.

Example of social engineering

A hacker pretended to be a representative of Chase Bank while saying that the action was needed on the target’s debit or ATM card. The attacker was trying to pressure the victim into divulging their information by leveraging their fear of not being able to access their money in their Chase account.

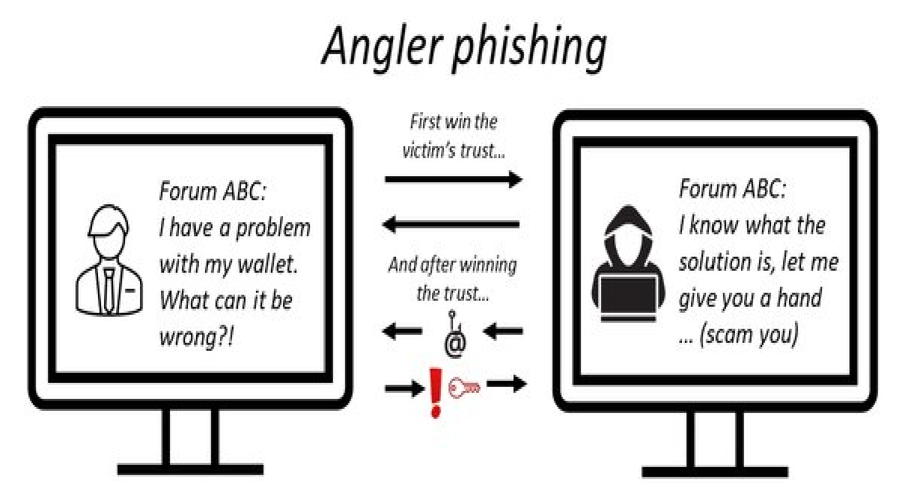


Angler phishing

Anglers use fake social media posts to get people to provide login info or download malware.

Example of angler phishing

Hackers pretended to represent Domino's Pizza on Twitter, fielding the concerns and comments of customers. Once they engaged with a customer, they would use their situation to try to get their personal information—using the guise of trying to get them a refund or a reward.

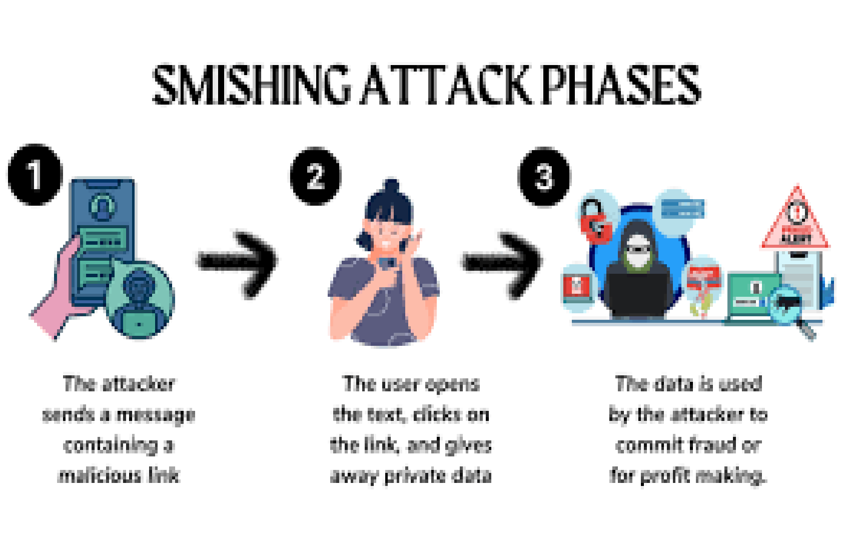

Angler phishing
Forum ABC:
I have a problem with my wallet. What can it be wrong?!
First win the victim's trust...
And after winning the trust...
Forum ABC:
I know what the solution is, let me give you a hand ... (scam you)

Smishing

Smishing is phishing through some form of a text message or SMS.

Example of smishing

Hackers pretended to be from American Express and sent text messages to their victims telling them they needed to tend to their accounts. The message said it was urgent, and if the victim clicked, they would be taken to a fake site where they would enter their personal information.

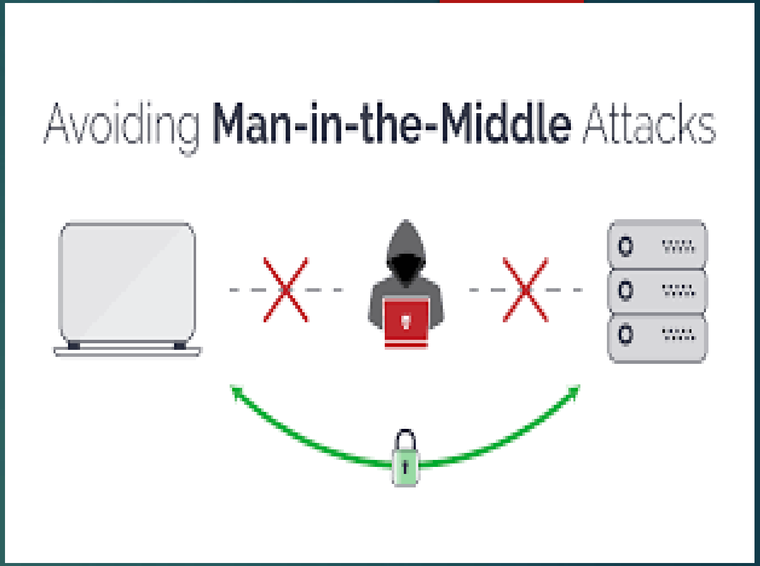

SMISHING ATTACK PHASES
1
The attacker sends a message containing a malicious link
2
The user opens the text, clicks on the link, and gives away private data
3
The data is used by the attacker to commit fraud or for profit making.

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.

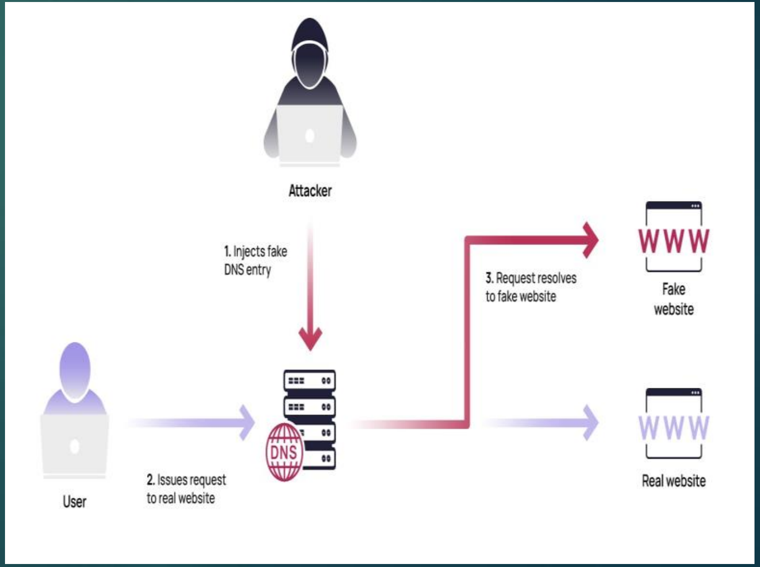


Website spoofing

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, also referred to as DNS spoofing, is when a hacker imitates the domain of a company—either using email or a fake website-to lure people into entering sensitive information. To prevent domain spoofing, you should double-check the source of every link and email.

Example of domain spoofing

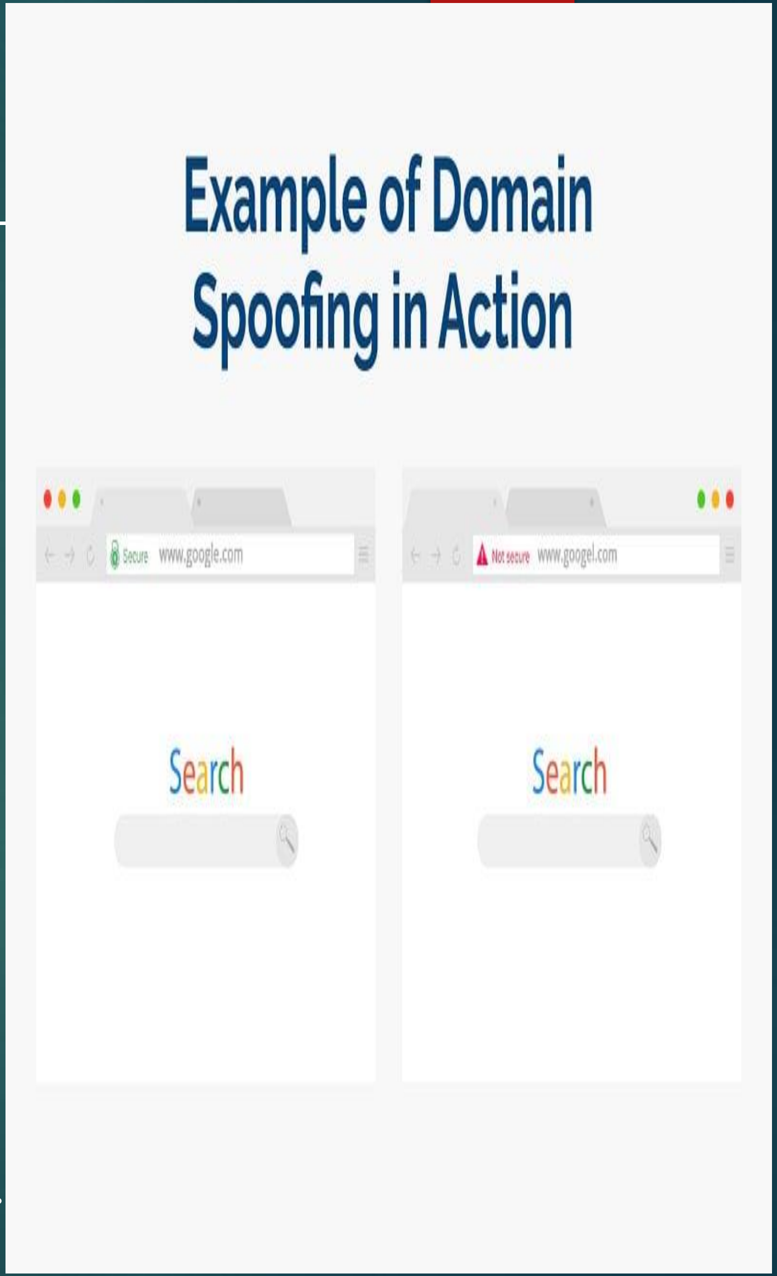
An attacker would execute a domain spoofing attack by creating a fraudulent domain made to look like a real LinkedIn site, for example. When users go to the site and enter any information, it is sent straight to hackers who could use it or sell it to someone else.

Image phishing

Image phishing uses images with malicious files in them meant to help a hacker steal your account info or infect your computer.

Example of image phishing

Hackers have made use of AdGholas to hide malicious code written in JavaScript inside images and HTML files. When someone clicked on an image generated by AdGholas, malware would be downloaded onto their computer that could be used to phish for their personal information.

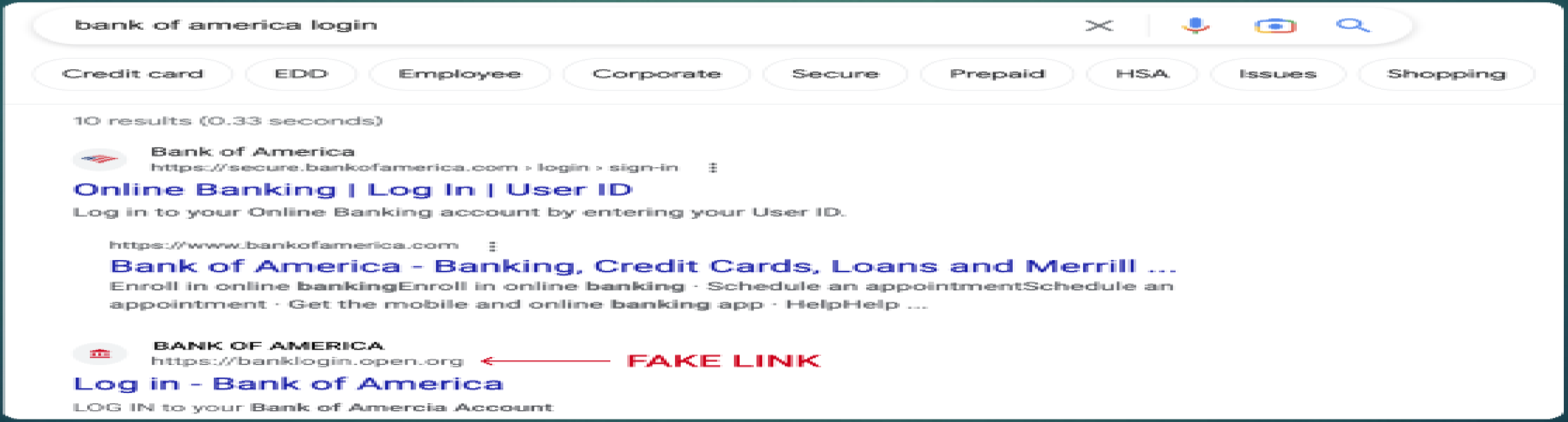

Example of Domain Spoofing in Action
Secure www.google.com
Search
Not secure www.googel.com
Search

Search engine phishing

A search engine phishing attack involves an attacker making fake products that look attractive. When these pop up in a search engine, the target is asked to enter sensitive information before purchasing, which then goes to a hacker.

Example of search engine phishing

In 2020, Google said that they found 25 billion spam pages every day, like the one put up by hackers pretending to be from the travel company Booking.com. An ad would pop up in users' search results that looked like it was from booking.com and included the site's address and the kind of wording users would expect from a real ad by the company. After users clicked, they were prompted to enter sensitive login information that was then transmitted to hackers.



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

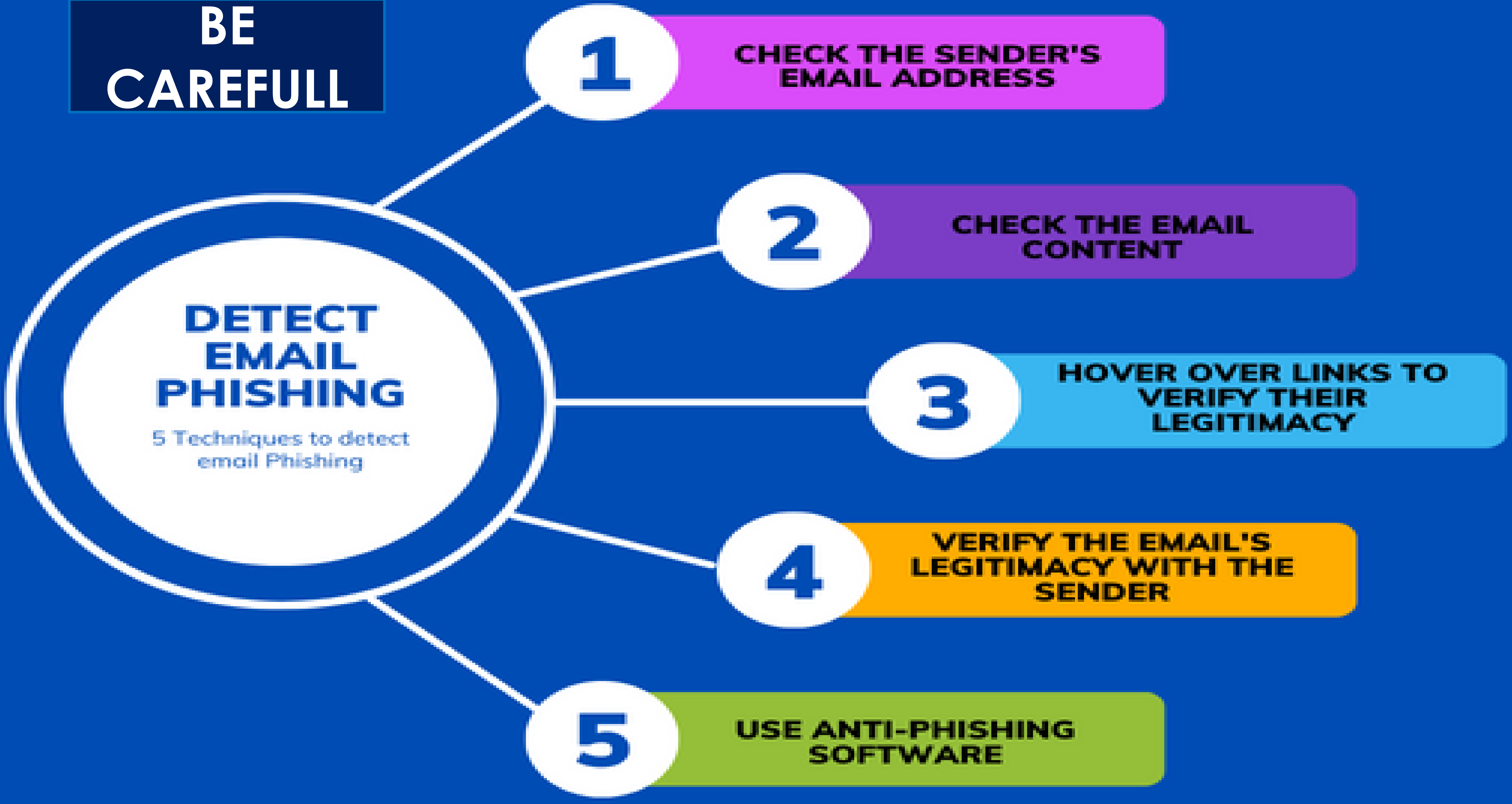
LOG IN to your Bank of Amercia Account

How To Spot Phishing Scams

Recognizing phishing attempts promptly is crucial for safeguarding your business's reputation and data security. Here are the key indicators of phishing attacks to watch for:

- **Urgent Action Demands**: Attackers exploit urgency to pressure recipients into hasty decisions before scrutinizing the email for inconsistencies
- **Poor Grammar & Spelling**: Phishing Emails often contain grammatical errors and spelling mistakes, unlike professionally crafted communications.
- **Unusual Greetings**: Formal greetings or unfamiliar phrases inconsistent with usual office communication style should raise suspicion.
- **Inconsistencies in Links, Addresses & Domains**: Hover over links to see where they go. Watch out for familiar names with strange domains or addresses - they might be trying to trick you.
- **Suspicious Attachments:** Most file sharing happens via trusted platforms. Double-check before opening anything unexpected, even from someone you know.
- **Too Good to Be True:** Beware of emails promising rewards or incentives, especially if the sender is unfamiliar or unsolicited.
- **Unexpected Requests:** Be wary of emails from managers or colleagues asking for personal info, even if they seem legit. Especially if they sound urgent!
- **Requests for Sensitive Information:** Be cautious with emails requesting sensitive data from unknown sources. Verify login pages to avoid falling for replicas.

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

- Advanced phishing attempts may come from email addresses that closely resemble legitimate ones. Always check for small inconsistencies, such as extra characters, domain mismatches, or foreign-language URLs. Sophisticated attackers may even attempt to compromise legitimate accounts and send phishing emails from within an organization's trusted network.

- Is the email asking for sensitive information or requesting urgent action? High-level phishing attempts often leverage authority, urgency, or emotional triggers (such as fear of financial loss or legal consequences) to compel users to act without thinking

- Phishers often clone the look of official emails with convincing logos, formatting, and even corporate jargon. Be cautious if any element—no matter how small—feels of

- Phishing campaigns often use a multi-vector approach, sending simultaneous emails, texts, or calls to increase the likelihood of success. Recognizing when multiple forms of communication arrive unexpectedly is a red flag.

Strategies for preventing a phishing attack

- Phishing awareness training will teach your employees what to look for, and what to do if they suspect a phishing attack is underway. According to research from Proofpoint published in 2022, 80% of organizations said that phishing awareness training reduced the employee's susceptibility to phishing attacks.
- Reinforce the awareness training with a simulated phishing attack. These show employees what a phishing attempt would look like in the real world, and how to apply the theory they've learned. According to research from the Infosec Institute, phishing simulations can double learning retention within 12 months. This means your employees are more vigilant against phishing attacks for longer
- Deploy an endpoint protection tool. These often include antiphishing features, including a blacklist of known phishing sites, network and device-wide monitoring, and email security tools that can identify suspicious messages and malicious links
- Implement verification policies for payments, so multiple people have to approve an invoice before wiring funds, and that payments are only made via approved channels. Attackers will often require payments in methods that are hard to trace or block, including gift cards and cryptocurrencies.
- Reduce your attack surface by embracing the Zero Trust concept of "least privilege access". By ensuring employees have the least amount of access required to do their job (or, put another way, they can only access the tools and systems they need, and nothing else), you limit the potential damage from a successful phishing attack.
- Adopt next-generation identity technologies like passkeys that support passwordless and phishing-resistant user experiences with 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 provides a higher return than you can get anywhere else.
- You have to make up your mind right away.
- You trust me, right?
- You don't need to check our company with anyone.
- We'll just put the shipping and handling charges on your credit card.

Tips to protect yourself from Phishing phone calls

- Don’t buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.

• Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups.

• Obtain a salesperson’s name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

• Don’t pay for a “free prize.” If a caller tells you the payment is for taxes, he or she is violating federal law.

• Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.

• If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.

Tips to protect yourself from Phishing emails

- I.T. will NEVER ask for your password over email. Please be wary of any emails asking for passwords. Never send passwords, bank account numbers, or other private information in an email.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. If you are not expecting an email with an attachment from someone, such as a fax or a PDF, please call and ask them if they indeed sent the email. If not, let them know they are sending out Phishing emails and need to change their email password immediately.
- Never enter private or personal information into a popup window.
- If there is a link in an email, use your mouse to hover over that link to see if it is sending you to where it claims to be, this can thwart many phishing attempts.
- Look for 'https://' and a lock icon in the address bar before entering any private information on a website.
- Look for spelling and bad grammar. Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have staff that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.

What to do when you think you received a phishing email

• First, do not click on any links within the email or download any attachment. Forward the email to abuse@valdosta.edu for Information Security to examine and determine if legitimate.

• If there is an attachment in the email, and you recognize the sender but aren't expecting an attachment from them, please call them and ask if it is legitimate.