

**PHISHING AWARENESS
TRAINING
CODE ALPHA CYBER SECURITY
INTERNSHIP PROJECT.**



First of all, we need to know what is phishing.

PHISHING:

Phishing is a type of cyber-attack where scammers send fake emails, messages, or websites to trick people into sharing their sensitive information, such as login credentials or financial details. It's like someone pretending to be a trustworthy person or company to trick you into revealing your secrets.



HOW DOES PHISHING WORK?

- The attacker sends deceptive emails, text messages, or links to counterfeit websites mimicking trustworthy sources like banks, social media platforms, or tech companies.
- The message often creates a sense of urgency or threat, like a warning that your account will be suspended unless you urgently click a link or share your login details.
- If you click the link or provide the information, the attacker can then exploit it to access your accounts, steal your identity, or engage in fraudulent activities.
- Phishing attacks may also involve malware, which is harmful software capable of infecting your device, leading to data theft or giving the attacker control over your computer

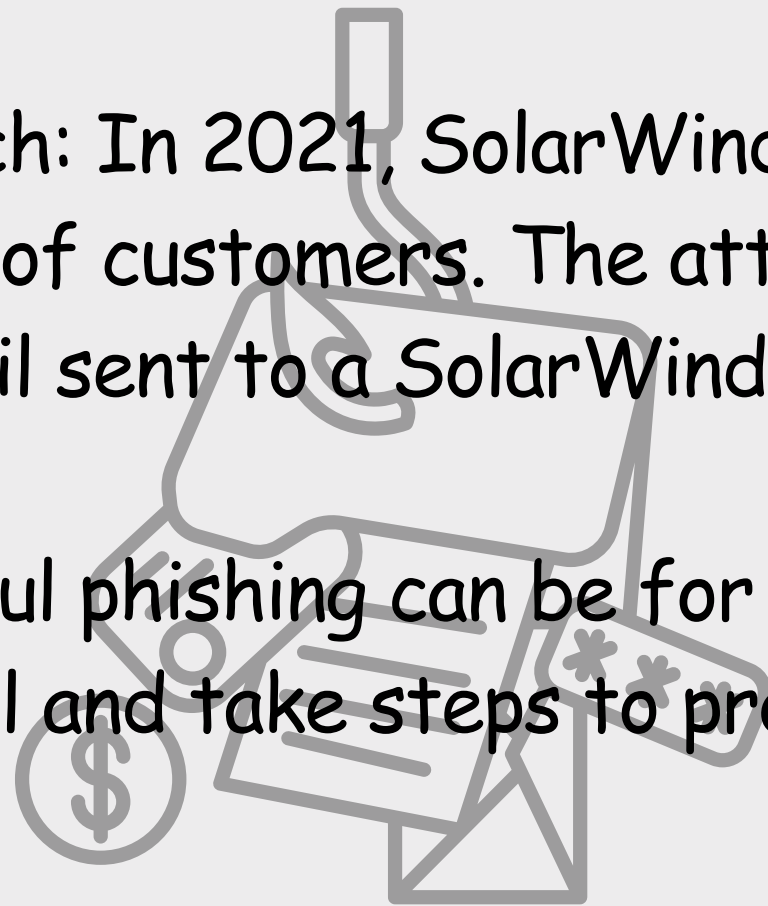
PHISHING ATTACKS.

In the past few years, there have been some big phishing attacks that caused a lot of harm. Here are a few examples:

- 2016 Yahoo data breach: In 2016, Yahoo said that all three billion of its user accounts were hacked. The attackers used phishing to steal user IDs and passwords, letting them get into the accounts.
- 2017 Equifax data breach: In 2017, Equifax, a big credit reporting company, got hacked, affecting over 143 million people. The attackers got sensitive info like Social Security numbers through a phishing email sent to an Equifax worker.
- 2018 Facebook data breach: In 2018, Facebook shared that personal info for up to 50 million users was stolen by attackers. They used phishing to trick users into giving up their login details, letting them access the accounts.

- 2021 SolarWinds data breach: In 2021, SolarWinds, a major software company, got hacked, affecting thousands of customers. The attackers got into the company's systems using a phishing email sent to a SolarWinds worker.

These examples show how harmful phishing can be for people, companies, and businesses. They also remind us to be careful and take steps to protect against phishing attacks.



HOW TO AVOID FALLING FOR PHISHING SCAMS

Hey there! If you're wondering how to protect yourself from phishing attacks, I've got some simple tips that can help you out. Check them out below!

Be Wary:

Don't trust unexpected emails, messages, or links, particularly if they request personal information. Verify their authenticity before clicking or responding. Phishing scams can be deceptive, but by being vigilant and double-checking, you can avoid becoming a victim. Stay secure online!

Check the Sender:

Look closely at the email sender's address. If it looks strange or doesn't match the usual emails from that person or company, be cautious.

Avoid Clicking:

Don't click on links or download attachments from unfamiliar or suspicious emails. It might be a trick to infect your device.

Verify Requests:

If you get a request for sensitive info, like passwords, from an unexpected source, verify it independently before sharing anything. Verifying can save you!

Use Security Software:

Keep your computer and devices protected with good security software. It can help catch phishing attempts and keep your information safe.

Enable Two-Factor Authentication (2FA):

Turn on 2FA for your accounts when possible. This adds an extra layer of protection even if your password is compromised.

Stay Informed:

Keep yourself updated on the latest phishing techniques. Knowing what to look for makes it easier to spot potential threats.

Educate Others:

Share these safety tips with friends and family. The more people know about phishing, the better we can all protect ourselves.

Remember, being cautious and informed is key to staying safe from phishing attacks.

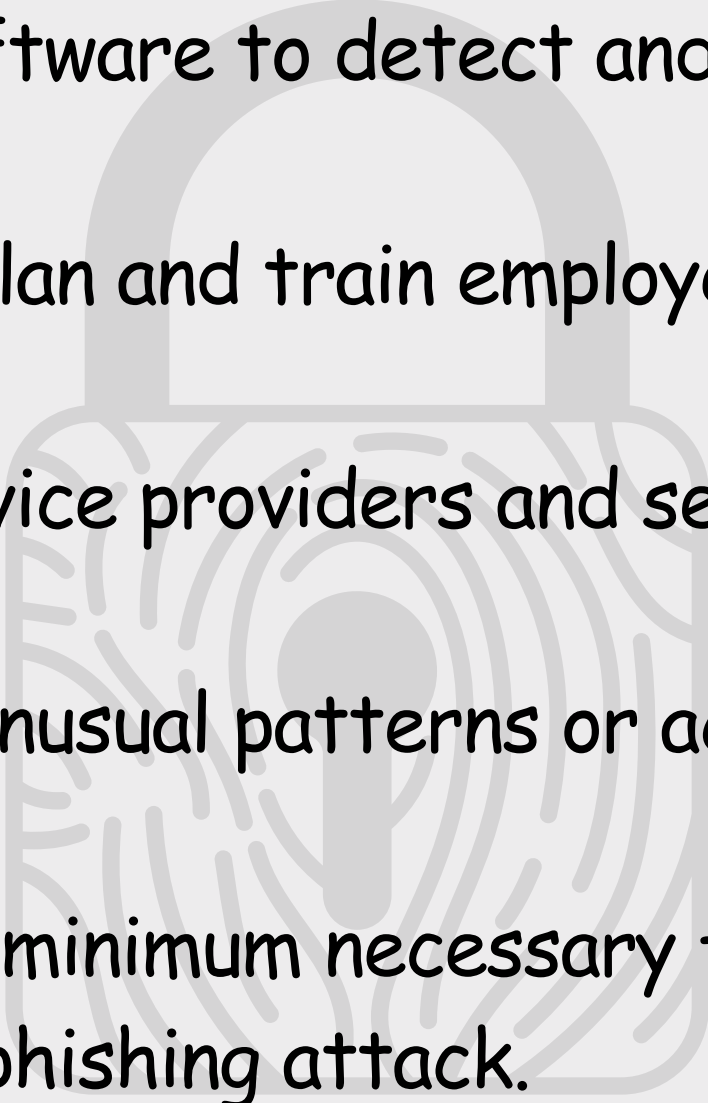
Stay Safe, Stay Secure!



How businesses can defend themselves against phishing attacks?


To protect against phishing attacks, businesses should:

1. Train employees to recognize phishing emails and avoid clicking on suspicious links or sharing sensitive information.
2. Use email filtering software to block phishing emails and advanced threat protection tools to detect malicious attachments or links.
3. Require multi-factor authentication to add an extra layer of security beyond passwords.
4. Keep software up to date with the latest patches to address vulnerabilities.
5. Use secure, encrypted connections (HTTPS) for websites and online services.
6. Conduct simulated phishing exercises to test employee awareness and address weaknesses.
7. Implement DMARC to prevent email spoofing and reject or quarantine suspicious emails.

- 
8. Deploy endpoint protection software to detect and block malicious activities on individual devices.
 9. Develop an incident response plan and train employees on how to respond to phishing attacks.
 10. Collaborate with internet service providers and security vendors to stay informed about phishing threats.
 11. Monitor network traffic for unusual patterns or activities that may indicate a phishing attack.
 12. Limit user permissions to the minimum necessary for their roles to reduce the potential impact of a successful phishing attack.

By following these measures and staying vigilant, businesses can significantly reduce the risk of falling victim to phishing attacks. Regular updates to security protocols and ongoing employee training are essential components of a comprehensive defense strategy.



The background is a light gray grid. It is decorated with various hand-drawn blue doodles. At the top, there are several overlapping circles and loops. On the right side, there are some star-like or burst-like shapes. At the bottom, there are more circles, a wavy line, and several small checkmarks or 'v' marks.

Thank you very much!

AMNA SADIA KORAI