Phishing Protection

Phishing is a type of online scam where attackers pretend to be legitimate companies or people to trick you into sharing private information like passwords or credit card details. This report explains the different types of phishing, ways to avoid it, and how to spot these scams.

What is Phishing?

Phishing is a trick where scammers pretend to be a trusted company or person to get you to share your private information. They use different methods to try and fool you, including:

- **Email Phishing**: This happens when you receive an email that seems like it's from a familiar company, but it's actually a fake.
1. **Spear Phishing**: Instead of sending the same message to a lot of people, scammers target specific individuals and use details about them to make the scam more convincing.
2. **Whaling**: This kind of phishing focuses on high-ranking people, like company leaders, to exploit their position and access to important information.
3. **Smishing**: Instead of using email, scammers send texts that contain harmful links or misleading instructions.
4. **Vishing**: Scammers make phone calls posing as real companies, asking for sensitive information.
5. **Clone Phishing**: A scammer copies a real email you've seen before but changes the links or attachments to include something dangerous.
6. **Angler Phishing**: This type of scam occurs on social media, using fake accounts to lure you into clicking harmful links.

How to Spot a Phishing Scam

- **Sense of Urgency**: The message may claim that something bad will happen, like your account getting closed, to make you react quickly without thinking.
- **Unusual Links**: Sometimes the links look almost correct but are slightly altered (for example, "amaz0n.com" instead of "amazon.com").
- **Unexpected Attachments**: If an email has an attachment you weren't expecting, be cautious because it could be harmful.
- **Bad Grammar or Spelling**: Scammers often don't bother checking their spelling or grammar, so the message might sound off.

How to Avoid Phishing

For Companies:

- **Train Employees**: Teach them how to spot phishing emails and practice with fake phishing tests.
- **Use Email Filters**: Set up filters that block suspicious emails.

- **Multi-Factor Authentication (MFA)**: Add an extra security step when logging in, like a code sent to your phone.
- **Limit Access**: Give employees access only to the information they need for their job.

For Individuals:

- **Double-Check Sources**: Before clicking, make sure the email or link is from a trusted source.
- **Use Antivirus Software**: This helps catch harmful attachments and links.
- **Enable MFA on Personal Accounts**: Use more than just a password for important accounts.
- **Avoid Public Wi-Fi**: Don't log into private accounts on public networks because they're not secure.

Detecting Phishing Scams

Common Methods:

- **Machine Learning**: This technology learns what phishing emails usually look like to spot them faster.
- **Heuristic Rules**: These rules look for unusual website names or specific phrases that are often used in phishing messages.
- **URL Checks**: Examine the link to see if the website is trustworthy by checking its age and reputation.
- **Content Filters**: These scan the content of messages for words or phrases that are frequently used in scams.

Tools to Help:

- **Email Security Programs**: Services that filter emails for suspicious content.
- **Web Filters**: Block access to known phishing sites.
- **Monitoring Systems**: Keep an eye out for unusual activity.
- **Device Protection**: Watch for signs of a compromised computer, like strange behavior.

What to Do If You Get Phished

1. **Disconnect Right Away**: If you think you've been phished, turn off the internet on the device to stop any harmful software from spreading.
2. **Report It**: Let someone in charge know what happened so they can take action.
3. **Change Your Passwords**: Update passwords for any accounts that might have been affected.
4. **Scan for Viruses**: Use antivirus software to check your computer for malware.

To sum things up, by being aware of phishing techniques, taking steps to prevent attacks, and knowing how to detect phishing, both organizations and individuals can protect themselves and reduce the risks of falling victim to these scams.