PHISING

Phishing is a form of cyber attack where attackers impersonate legitimate organizations or individuals to trick people into revealing sensitive information such as usernames, passwords, credit card numbers, or other personal details. This is usually done through deceptive emails, messages, or websites that appear to be trustworthy.

The most common type of phishing is email phishing, where attackers send emails that appear to come from trusted sources like banks, social media sites, or government institutions. These emails often contain urgent messages — such as account suspension warnings or security alerts — prompting the recipient to click on a malicious link or download a harmful attachment.

When the victim clicks on the link, they may be directed to a fake website that looks identical to the real one. Once the victim enters their login credentials or personal details, the attackers capture that information and use it for identity theft, financial fraud, or further attacks.

Phishing can also occur via SMS (smishing), voice calls (vishing), or even social media. Attackers continuously evolve their techniques, making phishing attempts more convincing and harder to detect.

To prevent phishing, users should be cautious of emails or messages that ask for personal information, especially if they contain grammatical errors, unexpected attachments, or mismatched URLs. Hovering over links before clicking, verifying sender email addresses, and using two-factor authentication are effective practices.

Organizations also implement spam filters, anti-phishing software, and employee awareness training to reduce the risk.

Phishing remains one of the most common and dangerous cyber threats because it exploits human trust. Education and vigilance are key to defending against it.

In summary, phishing is a deceptive method used by cybercriminals to steal confidential information. Recognizing the signs and taking preventive measures can protect individuals and organizations from serious harm.

TYPES OF PHISING

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | Type | Channel Used | Target Level |  |
|  |  |  |  |  |
|  | Email | Email | General users |  |
|  | Spear | Email | Specific individuals |  |
|  | Whaling | Email | Executives/CEOs |  |
|  | Smishing | SMS | Mobile users |  |
|  | Vishing | Phone calls | General users |  |
|  | Clone | Email | Existing email chain |  |
|  | Angler | Social Media | Public users |  |

How to Stay Safe from Phishing

* **Never click suspicious links** in emails, SMS, or pop-ups.
* **Check the sender’s email address** carefully (look for typos or fake domains).
* **Hover over links** before clicking to verify the actual URL.
* **Enable Two-Factor Authentication (2FA)** for all important accounts.
* **Don’t share passwords, OTPs, or PINs** via email or message.
* **Avoid downloading attachments** from unknown or untrusted sources.
* **Use strong spam filters** to block phishing emails automatically.
* **Install antivirus and anti-phishing software** and keep it updated.
* **Use browser security extensions** (e.g., Bitdefender, Netcraft).
* **Use a password manager** to avoid typing passwords on fake sites.
* **Update your system and browser** regularly to fix security bugs.
* **Educate yourself and others** about phishing signs and tactics.
* **Report phishing attempts** to your email provider or security team.
* **Avoid logging in through links sent via messages** — visit sites directly.
* **Be cautious of emails that create urgency**, threats, or offer prizes.