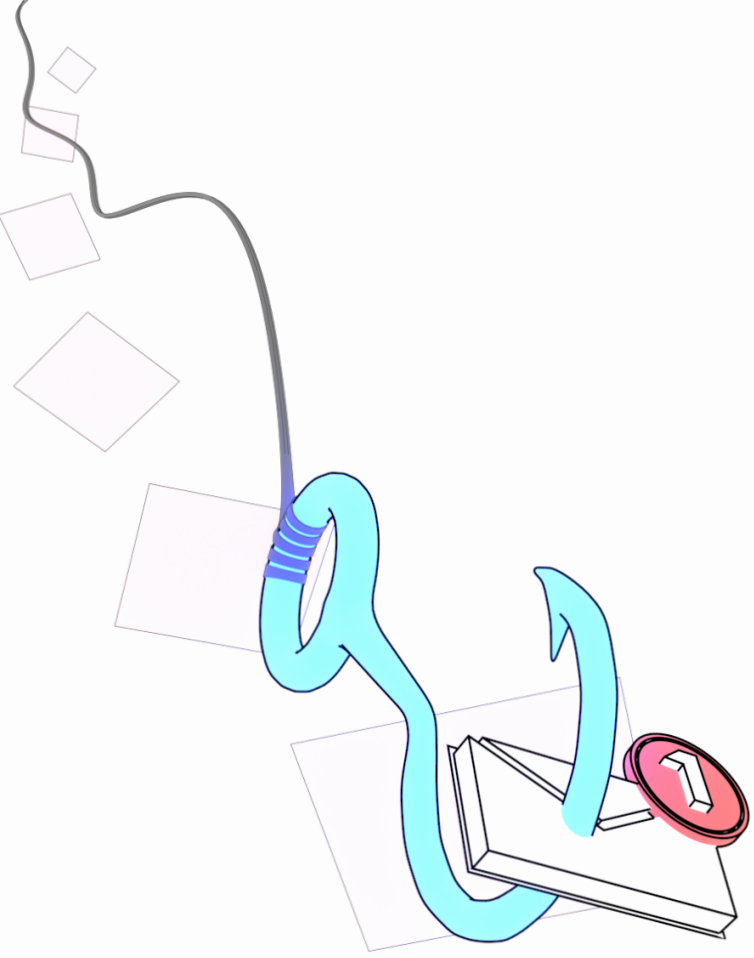
Watch for These

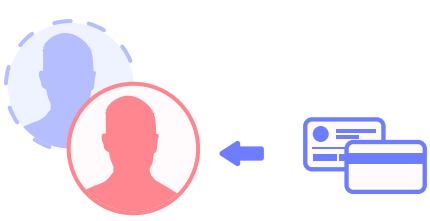
6 Phishing Scams

Phishing is a type of cyber fraud that utilizes deceptive emails or other electronic communication to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. While emails are the most common delivery method of phishing attempts, cybercriminals may also use:

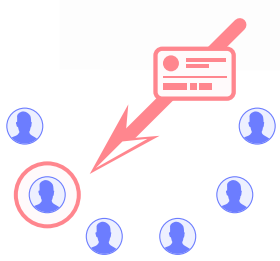
- **Voicemails**
- **Live phone calls**
- **Text messages**
- **Fake or misleading websites**
- **Social media messages**



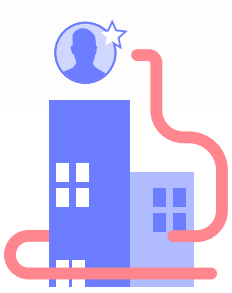
Here are **six of the most common types of phishing scams** to watch out for:



Deceptive phishing is when a cybercriminal impersonates a recognized sender to steal personal data and login credentials.

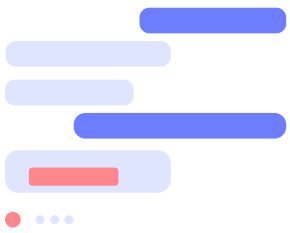


Spear phishing is typically aimed at specific individuals or companies by using personalized information to convince victims to share their data.

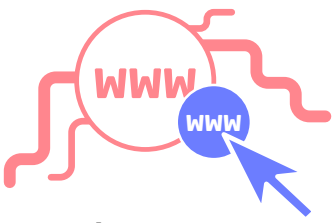


Whaling aims to trick high-profile targets such as CEOs, CFOs and COOs into revealing sensitive information, like payroll information or intellectual property.

Vishing is sometimes called "voice phishing" and occurs when a criminal calls a target's phone to get them to share personal or financial information.



Smishing refers to "SMS phishing" and incorporates malicious links into SMS text messages.



Pharming redirects a victim to a site of the cybercriminal's choosing by installing a malicious program onto their computer.

To protect against all types of phishing scams:

Remain informed about phishing techniques.

Examine a message before clicking.

Back up data regularly.

Never give out personal information.

Use antivirus software.

Keep computer systems up to date.

Phishing scams are becoming **more sophisticated and severe**. By taking the proper precautions, organizations can minimize their damage.