shield your loved ones: a guide to spotting and preventing phishing scams

44% of people consider a branded email safe, but over 30 million malicious messages in 2022 used Microsoft branding or similar imagery.

Phishing is when an attacker sends a fraudulent message designed to trick a person into revealing sensitive information.

They are successful because they are simple.

Attackers usually disguise themselves as a known business or service to gain victim's trust. They often use a sense of urgency to get people to act quickly, before they can realize it is a scam.

Real life examples of phishing attacks:

- How a 'Shark Tank' Star became the victim of a phishing scam (video)
- Netflix phishing scam targets 110 million subscribers

Protect yourself and loved ones from phishing attacks. Learn about the tactics hackers use to trick their victims and how to spot the signs in this guide.

Allstate cybersafety

Allstate®

shield your loved ones: a guide to spotting and preventing phishing scams

Phishing tactics: *how hackers trick their victims*

Smishing (text message phishing)

Tricks victims into thinking they've received a message from a trusted person or organization that already has their phone number and information.

Telephone oriented attack delivery

"Vishing" is when hackers call posing as a legitimate company to extract personal information. Recently, they've started sending emails that prompt victims to call back, creating a false sense of security.

Website spoofing

Hackers create fake websites with legitimate branding to collect your information when you log in.

Search engine phishing

Hackers manipulate search engines to include fraudulent websites.

Pop-up phishing

Pop-up phishing tricks you into clicking on a fake security alert or issue, leading you to download malware or call a fake support center.

Social media phishing

Using fake social media posts is a rising trend among hackers on sites like Facebook, Twitter, LinkedIn and more.

Know the signs: *how to spot a phish*

Generic greeting or signature

In most circumstances, legitimate emails that you receive should be addressed to you directly.

An appeal to your curiosity or helpful nature

Common scams include emails claiming that you've won a prize or are eligible for a prize if you give them your information, or emails claiming to be from a charitable organization in times of crisis or tragedy.

Information requests

Personal information requests should be viewed with suspicion, as genuine banks or institutions do not ask for personal details via email or text messages.

Urgency or threat

Urgency or consequences can cause hasty action without proper investigation. When receiving an email that demands immediate action, it is important to take a moment and consider if it could be a scam.

Hyperlinks and attachments

Be suspicious of hyperlinks included in emails, especially if the email is from an unknown source.

Also be wary of email attachments, especially .zip or .exe files. Confirm via another means (phone call or IM) if the attachment is safe to open.

Never open an email attachment or link that you are unsure about.

Sender email address

Use caution if you don't know the sender or you weren't expecting the message. Check the 'from' address carefully, hackers can imitate a company by using simple misspellings (ex. barclaya.net instead of barclays.net) or use of a special character (ex. ņordvpn.com instead of nordvpn.com).

Allstate cybersafety

Allstate®