Phishing attacks are scams designed to gain access to your system by fraudulently obtaining your log-in credentials, steal your identity, or get you to send money to criminals fraudulently responding to an email, clicking on a link, or downloading an image the fraud victim can trust. Their attackers can lead to leaked confidential information, infected networks, financial demands, corrupted data, or worse.

Here is how to avoid becoming a phishing victim:

1. Inspect the sender’s email address closely. Look for small changes signaling a fake identity.

2. Be wary of emails that utilize a generic greeting, asking you to act urgently.

3. Look for verifiable sender contact information. If in doubt, do not reply. Start a new email to respond.

4. Use the phone to convey private information. Never send sensitive information via email.

5. Avoid clicking on unexpected links. Go to the official website and log in instead.

6. Avoid opening email attachments from unknown senders or even friends who do not normally send you attachments.

7. Install a phishing filter for your email account.

Learn more on how to avoid being a phishing victim.

Get the latest news from Microsoft Security: go to microsoft.com/en-us/securitynow.

Share this infographic: 

Read the rest of the series here:

- 10 easy rules to secure your personal data & protect your devices
- Protect your business: Cybersecurity 101
- 5 pro tips to protect yourself from tech support scams

©2021 Microsoft Corporation. All rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.