baramundi

BARAMUNDI CHECKLISTS provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: www.baramundi.com/checklists

Phishing attacks – 5 strategies for prevention

The word "phishing" uses the first letters in the words "password harvesting" in place of the 'f' in "fishing." It refers to text, voice or email messages from hackers disguised as known contacts or institutions asking victims for sensitive account information or electronic funds transfers. But how can phishing attempts be recognized and stopped before damage occurs?

Sender's address

Check whether the sender's address or number matches a known and verified contact. Spelling, grammatical and other errors are warning signs.

Domain name

Always check what comes after the @ in the sender's email address. Addresses with typos or modified spelling that resembles a legitimate address are common deceptions.

Spoofing

Criminals often send messages that use the name and address of a legitimate contact – even your own! That's why you can't rely only on names or addresses that seem to be correct. Careful reading of message content can help. Technical measures such as checking the Reply-to, server, authentication, routing and other data in an email header can help determine if a message is bogus or legit.

Dangerous links and attachments

Phishing often tricks victims into downloading malware via links or document attachments. Always view the URL embedded in the text or graphics of a message before clicking on it by placing the cursor over it for a few seconds. Do not click on an attachment unless you requested or expected it and are 100% sure it's safe.

Verify

Phishing exploits victims' trust and fear. It is far safer to verify any suspicious text, voice, or email message by using a separate trusted web address or telephone number to contact the sender. Businesses and government agencies are aware of phishing attacks and want to help people avoid scams.

> **In short: Phishing attacks pose a significant risk. While attentive employees are critical in the effort to identify dangerous links, everyone should receive ongoing cybersecurity awareness training. The baramundi Management Suite also plays a key role in securing systems by enabling rapid and efficient distribution of regular updates and security patches to eliminate vulnerabilities.**