TRAVA CHECKLISTS

Phish-Proof Tips: Outsmarting Sneaky Scammers

Phishing emails typically tell a story to get you to take an action: clicking a link, entering personal information, opening a communication channel with the attacker. **It is important to understand what you are being asked to do and whether this behavior is expected.**

There are things you can do the next time you get an email to protect yourself and your organization from being compromised. Emphasizing a few simple practices to improve your cyber hygiene will put you on the path to becoming a cybersecurity superstar!

□ **Check for Grammatical and Punctuation Errors:** Take note of emails that contain poor grammar or punctuation errors. These mistakes are often indicators of phishing attempts, as legitimate organizations typically maintain professional communication.

□ **Evaluate the Content and thee Call to Action:** Phishing emails often rely on social engineering tactics to manipulate emotions and prompt immediate action. Be cautious of emails that:

- Create a sense of urgency with deadlines and warnings.
- Request sensitive information such as passwords or personal data.
- Promise unbelievable rewards or unsolicited offers.

□ **Verify the Link Before Clicking:** When an email includes links or buttons, hover your mouse pointer over them to preview the destination URL. URLs should correspond to a trusted domain before clicking.

□ **Beware of Shortened Links:** Cybercriminals often use URL shortening services to hide the actual destination. Verify the legitimacy of a shortened link—hover over it to reveal the true URL before.

□ **Examine the "From" Address:** While the sender's name may appear legitimate, verify the sender's email address and domain to ensure it matches previous trusted communication.

□ **Communicate with Your Team:** Encourage open communication among coworkers regarding suspicious emails. Sharing observations and discussing potential threats collectively can prevent adverse outcomes.

□ **Visit Websites Directly:** Instead of clicking on email links, use your web browser to navigate directly to the website of vendors or service providers. This approach enhances security by providing information on trusted sites and validating the email's authenticity.

travasecurity.com

Cybersecurity doesn't have to be complicated. **We'll prove it.**

TRAVA

Stellar product.
Better people.