Security Hints + Tips

April 1, 2024

Don’t Be Fooled by Workspace Tools

Many organizations use platforms such as Microsoft Teams, Google Drive, or Zoom to stay connected. Unfortunately, these trusted communication tools can lead to a false sense of security. Just like with traditional email, bad guys can use these platforms to launch a cyber attack. Below are three examples of how cybercriminals use these platforms for phishing—and what you can do to keep your organization safe

Lurking

Recently, a cybercriminal gained access to an organization’s Microsoft Teams channel, which is similar to a group message or a chat room. The scammer lurked in the channel for nearly a year, reading messages, collecting data, and waiting for the perfect time to strike. Finally, someone asked that a file be shared to the channel and the bad guy used this opportunity to send a malicious ZIP file. When opened, the file installed malware that gave the scammer full access to the victim’s computer.

Remember: If someone sends you a link or an attachment, verify that you know and trust the sender before you click.

Playing Tag

On Google Drive, anyone can be tagged in a file, so long as their Gmail address is valid. This means that if a bad guy tags you in a Google document, you will receive a legitimate notification from Google that includes a link to the bad guy’s file. If you view the bad guy’s file, you’ll likely find that it tells you to click another link. This second link is actually a malicious attempt to steal your sensitive information.

Remember: If you receive a suspicious notification, contact your IT department or follow the specific security procedure for your organization.

Phony Notifications

Attending meetings on Zoom is as simple as clicking a button within an email. Unfortunately, getting phished is just as easy. Cybercriminals send out fake Zoom notifications that claim you missed an important meeting. They use a sense of urgency to get you to click on a link to view the meeting schedule. But don’t be fooled! The link actually sends you to a phony login page designed to steal your username and password.

Remember: If an email asks you to log in to an account or online service, log in to your account through your browser—not by clicking the link in the email.

The KnowBe4 Security Team
KnowBe4.com