Cyber Risks

Phishing Attacks on Business Smartphones Grow

PHISHING ATTACKS on enterprise and employees' smartphones continue plaguing businesses, with attacks increasing 10% in 2022 from 2021, according to a new report.

As more businesses have adopted bring-your-own-device (BYOD) policies, the risks grow for these attacks, which can be costly.

Last year, 11.8% of mobile enterprise users clicked on six or more malicious links, compared with just 1.6% in 2020, which "indicates users are having a tougher time recognizing phishing attempts," according to the report by cyber security firm Lookout Inc.

What is phishing?

Phishing attacks try to coax a target to reveal personal information like passwords or credentials in an e-mail that looks like it's been sent from a reputable source.

Messages are often enticing or convey a sense of urgency.

Typical Phishing Topics

- Prize notifications
- Tech support notifications
- Shipping notifications
- Contact-tracing messages that request personal information.

The dangers

Successful phishing attacks can have costly implications for a business, including:

Rerouting payments – Attackers gain access to your accounts so they can reroute legitimate vendor payments to their own accounts by modifying invoices. They may also gain access to an employee's e-mail and impersonate them, modify content of e-mails and request funds.

System outage – If the phishing attack is a ransomware attack, it can shut down your entire database and website. Depending on how much you rely on your systems, the damage could be a few hundred dollars or tens of thousands in lost revenue.

Data theft – A phishing attack can also result in sensitive company data being compromised or stolen. If personal data is exposed, it could have regulatory consequences, including fines.

What you can do

There are steps you can take to protect your organization, its company-owned and BYOD devices from phishing attacks. Cyber security firm TechTarget recommends:

Using mobile security tools – Security solutions called endpoint management tools may add a layer of protection to mobile devices. These include:

- Symantec Endpoint Protection Mobile
- Trend Micro Mobile Security
- Kaspersky Endpoint Security
- Microsoft Intune
- F-Secure Mobile Security.

Other solutions that can filter out spam text messages and block known sources of phishing attacks include:

- RoboKiller
- Apple iPhone built-in spam filters
- SpamHound SMS Spam Filter.

Creating mobile device policies – Establish smartphone policies for your employees to follow. If you have an IT person, they can set up these policies through mobile device management tools like Microsoft Intune or MobileIron.

These tools can keep employees from responding to messages from unknown sources or clicking on links send via text messages. They can also block messages from unknown sources.

Training your employees – Train your employees to not click on links in messages from unknown sources and to be wary if a co-worker is asking them to click on a link.

Provide examples of how to identify phishing attacks, what actions to take if they receive a request for information, and how to check that the mail is from a trusted source. ❖