## Phishing Attacks on Business Smartphones Hit Record Levels

Phishing attacks on enterprise and employee-owned smartphones increased 10% in 2022, according to a new report highlighting the continuing and growing risk of these attacks.

As more businesses have adopted bring-your-own-device (BYOD) policies, the risks grow for these attacks, which aim to get the phone user to click on a link that releases malicious code.

The risks for business if a phishing attack is successful on one their employee's or company-supplied smartphones are many, including the hackers rerouting payments to their own accounts, accessing sensitive company data or employees and customers' personally identifiable information, or data loss.

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 is an attempt to coax a target to click on a link in an e-mail that looks identical to real ones from banks and other legitimate sources. Often these links will direct them to a website that looks like one they already use in hopes they'll enter their username and password. Or the link will release code onto the phone.

Messages can be enticing or convey a sense of urgency, such as

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

### The dangers

Successful mobile 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**

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

**Using mobile security tools** — There are new security solutions called endpoint management tools that add another layer of protection to mobile devices that connect to your database. 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 use policies** — Establish enterprise 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 will implement policies prohibiting employees from responding to messages from unknown sources or clicking on links sent via text messages. They can also block messages from unknown sources.

**Training your employees** — The weakest link in your defenses is your own employees and the risk of them clicking on a malicious link in a text message or e-mail.

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.

*This material was created by Insurance Newsletters and authorized for use by Brown & Stromecki Agency

###