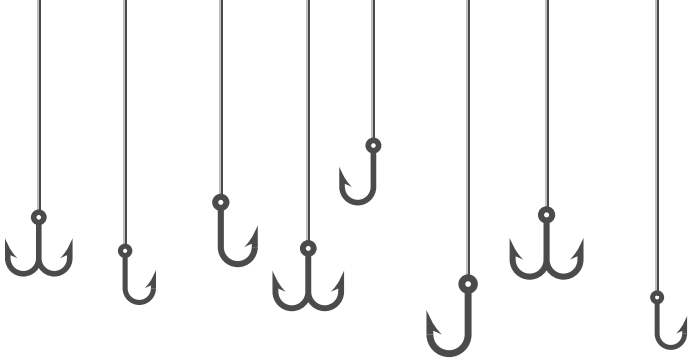
MobileIron Threat Defense

DETECT AND REMEDIATE AGAINST MOBILE PHISHING ATTACKS

mobileiron



PHISHING

Phishing has been a threat for at least a quarter of a century, but the ascendance of mobile has given phishing new life. With mobile usage now surpassing desktop usage, particularly among enterprise users, cybercriminals see mobile as a prime target for phishing attacks.

Phishing attacks directed at mobile devices are rising some 85 percent per year. Innovative phishing attacks now simulate mobile browser information, including animations, for popular sites like Airbnb and Facebook, in a bid to capture vital information from unsuspecting users . According to Verizon, over 90% of breaches start with a phishing attack... and with more than 60% of emails being read on mobile, mobile phishing is a major issue.

Aside from the sheer volume of mobile users available as targets, cybercriminals find mobile users to be particularly enticing. The reasons for this all comes down to, as Verizon also observed in their annual data breach report, one basic fact: Mobile technology lends itself to phishing in ways that traditional desktop technologies do not.

Top 10 reasons mobile technology is **Phishing-phriendly**

Users are in Charge

Users typically administer their own devices, lacking the automated patching and updating processes that corporate desktops and laptops have

Tiny Screens

Small screen size makes it more difficult to access and view key information

OSs, Apps are Great Hiding Places

OSs and apps limit the availability of information needed to properly assess the authenticity of emails, web pages, etc.

Users Trust Too Much

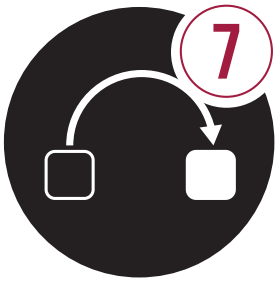
Users feel a personal connection to their mobile devices that fosters unfounded trust in the device and the content on it

No Side by Side View

Viewing web pages and other data in screens side-by-side is difficult or impossible

Look Before You Tap

User interface limits the amount of available information while prompting users to make fast decisions



Gotta Toggle

Moving between web pages or between apps requires toggling

Texts = Urgent

Users view SMS as more urgent and so can be less inclined to verify requests sent via SMS

Don't Ask, Just Tell

GUI design encourage actions such as accept, reply, send, like, etc., facilitating user responses to requests

Texting While Distracted

Users use mobile devices while walking, talking, driving, etc., and can receive and respond to requests while distracted, without having to view the originating app, making it more likely they will accept the request

Phishing's danger to the Enterprise

Phishing attacks are often targeted at the enterprise, with devastating results.

$1.4 Million

Average cost to the enterprise of a phishing attack[7]

85%

Number of organizations that have experienced phishing and social engineering attacks[8]

98%

Number of enterprise attacks that had no malware and were instead credential theft and email scams[9]

1 in 3

Number of successful breaches—those with a confirmed disclosure of data to an unauthorized party—involved phishing[10]

78%

Number of cyber-espionage incidents that involved phishing[11]

DEFENDING AGAINST MOBILE PHISHING

The first line of defense against mobile phishing is education. The more that mobile users know about phishing attacks, and how to avoid them, the better. But education is not enough. Protecting mobile devices against phishing attacks requires a combination of approaches.

To protect against the most attacks, MobileIron Threat Defense (MTD) includes both deterministic and machine learning-based anti-phishing protection. MTD checks any links (in an email, text, social media or messaging app) against a continuously updated global database of malicious phishing URLs. To protect user privacy, MTD does not read or parse the messages themselves. By default, MTD alerts the user if the URL is malicious prior to the connection being completed.

At the same time, MTD employs machine learning-based phishing detections. Critically, this detection occurs on-device, and does not require network access. Users therefore receive protection even from previously unknown phishing sites that are not yet on any known list.

SUMMARY

Mobile phishing is top of mind for enterprise security professionals. Defending mobile users and their devices against phishing is fast becoming a top priority. If you are interested in learning more about the ways MTD can help protect your enterprise against mobile phishing, please contact us. Our mobile security experts are standing ready to help.

ABOUT MOBILEIRON

MobileIron is redefining enterprise security with the industry's first mobile-centric, zero trust platform built on the foundation of UEM to secure access and protect data across the perimeter-less enterprise. Zero trust assumes that bad actors are already in the network and secure access is determined by a "never trust, always verify" approach. MobileIron goes beyond identity management and gateway approaches by utilizing a more comprehensive set of attributes before granting access. A mobile-centric, zero trust approach validates the device, establishes user context, checks app authorization, verifies the network, and detects and remediates threats before granting secure access to a device or user. The MobileIron security platform is built on the foundation of award-winning and industry-leading UEM capabilities with additional zero trust-enabling technologies, including ZSO, MFA, and MobileIron Threat Defense (MTD). Over 19,000 customers, including the world's largest financial institutions, intelligence agencies, and other highly regulated companies have chosen MobileIron to enable a seamless and secure user experience by ensuring only authorized users, devices, apps, and services can access business resources.

TAKE THE NEXT STEP

Find out how MobileIron can help you securely transform your critical business processes with our proven, industry-leading UEM platform and professional services.

Please visit us at www.mobileiron.com

Sources

1. Phishing.org. History of phishing. http://www.phishing.org/history-of-phishing

2. Statcounter. Desktop vs Mobile vs Tablet Market Share Worldwide
   Desktop vs Mobile vs Tablet Market Share Worldwide. Apr 2018 - Apr 2019. Data cited from May 2019. http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

3. Cyberscoop. Phishing attacks against mobile devices rise 85 percent annually. April 2018. https://www.cyberscoop.com/phishing-attacks-mobile-devices-lookout/

4. The Hacker News. BEWARE – New 'Creative' Phishing Attack You Really Should Pay Attention To. March 2019. https://thehackernews.com/2019/03/ios-mobile-phishing-attack.html

5. Verizon. 2019 Data Breach Investigations Report. May 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

6. Ibid.

7. Ibid.

8. Accenture. Ninth Annual Cost of Cybercrime Study. March 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

9. PhishLabs. 2019 PHISHING TRENDS AND INTELLIGENCE REPORT. April 2019. https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf

10. Verizon. 2019 Data Breach Investigations Report. May 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

11. Ibid.