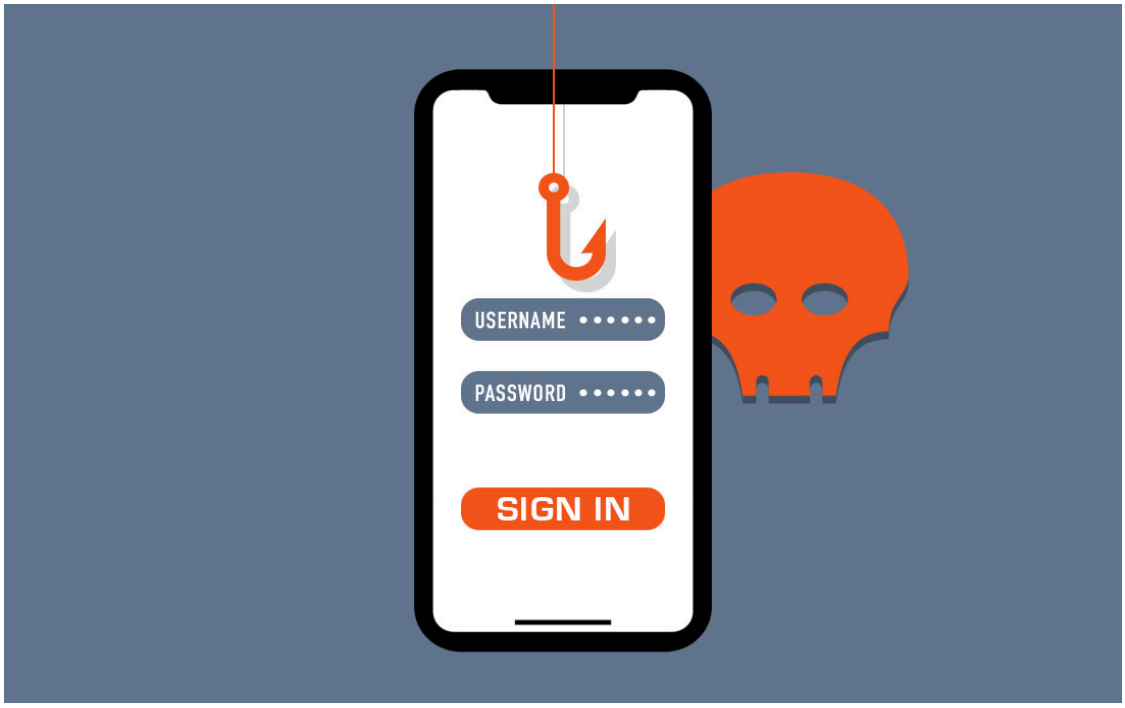
ZIMPERIUM®
MOBILE THREAT DEFENSE

Zimperium Mobile Phishing Solutions for Government

PHISHING

Phishing[1] has been a threat for at least a quarter of a century, but the ascendance of mobile in the public sector has given phishing new life. With mobile usage now surpassing desktop usage[2], cybercriminals see mobile as a prime target for phishing attacks.

Phishing attacks directed at mobile devices are rising some 85 percent[3] per year. The Department of Defense reported that 8 out of every 10 inbound emails to the department had to be blocked[4], while the Pentagon had calculations showing an anticipated 13 billion emails in a single year[5]. According to Verizon[6], over 90% of breaches start with a phishing attack. With more than 60% of emails being read on mobile, mobile phishing is a high-stakes 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, as Verizon also observed in their annual data breach report[7], to 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

#1: Users are In Charge

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

#2: Tiny Screens

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

#3: 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.

#4: 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

#5: No Side by Side View

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

#6: Look Before You Tap

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

#7: Gotta Toggle

› Moving between web pages or between apps requires toggling

#8: Texts = Urgent

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

#9: Don't Ask, Just Tell

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

#10: 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 IS INCREASING

Phishing attacks are becoming more sophisticated and frequent.

- **34 Million per day**
  Number of malware-infested emails that the Department of Defense alone reported receiving[8]

- **1 in 3**
  Number of employees at one federal agency that failed a phishing test[9]

- **98%**
  Number of phishing attacks that had no malware and were instead credential theft and email scams[10]

- **1 in 3**
  Number of successful breaches–those with a confirmed disclosure of data to an unauthorized party–that involved phishing[11]

- **78%**
  Number of cyber-espionage incidents that involved phishing[12]

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, Zimperium zIPS includes both deterministic and machine learning-based anti-phishing protection. zIPS 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, zIPS does not read or parse the messages themselves. By default, zIPS alerts the user if the URL is malicious prior to the connection being completed.

At the same time, Zimperium's z9 engine 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 public sector IT 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 Zimperium can help protect your agency against mobile phishing, please contact us. Our mobile security experts are standing ready to help.

ZIMPERIUM®

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] Department of Defense. Norton: Secure, operate, and defend are the fundamentals. https://www.disa.mil/NewsandEvents/2017/AFCEA-Luncheon
[5] Inc. Government Agencies Are Under Siege From Phishing Attacks. Could Your Company Be Next? https://www.inc.com/adam-levin/government-agencies-are-under-siege-from-phishing-attacks-could-your-company-be-next.html
[6] Verizon. 2019 Data Breach Investigations Report. May 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[7] Ibid.
[8] Inc. Government Agencies Are Under Siege From Phishing Attacks. Could Your Company Be Next?
https://www.inc.com/adam-levin/government-agencies-are-under-siege-from-phishing-attacks-could-your-company-be-next.html
[9] FCW. 1 in 3 FHFA employees failed phishing testFeb 2019. https://fcw.com/articles/2019/02/11/cyber-phishing-oig-fhfa.aspx
[10] PhishLabs. 2019 Phishing Trends and Intelligence Report. April 2019. https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf
[11] Verizon. 2019 Data Breach Investigations Report. May 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf