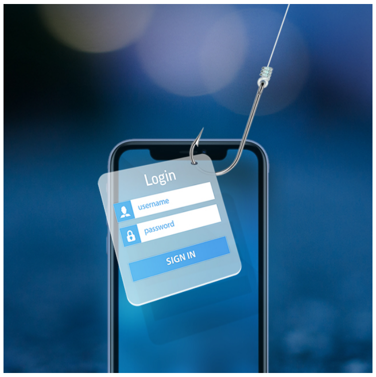
ZIMPERIUM®
ADVANCED MOBILE SECURITY

Mobile Phishing Takes the Path of Least Resistance

Enabling Enterprises to Effectively Manage Mobile Risks

Phishing[1] has been a threat for at least a quarter of a century, but the COVID-19 pandemic tripled the frequency of phishing attacks in 2020 alone. And this number is only going to continue to rise. With mobile endpoints surpassing desktop use[2], cybercriminals see mobile as a prime target for phishing attacks.

The Department of Defense reported eight out of every ten inbound emails to the department had to be blocked[3]. In comparison, the Pentagon had calculations showing an anticipated 13 billion emails in a single year[4]. And according to Verizon[5], over 90% of breaches start with a phishing attack.



Mobile endpoints are no longer personal-only devices and have been adopted into the enterprise through bring your own device (BYOD) policies and enterprise-focused applications for everything from identity verification to data access. With this adoption, IT teams often deploy enterprise-only applications with limited security controls to support the roaming data access points. But this scope of the security controls focuses on enterprise applications, leaving high-use consumer apps unprotected against attack. Simply put, cybercriminals target personal email, SMS, and personal messaging apps as unprotected entry points into enterprise data.

Through 2020, 87% of enterprises reported dependence on their employee's ability to access mobile business apps from their mobile device[6], and over **60% of all emails, business and personal, were accessed on mobile devices**[7]. Pair this with the fact that more than 52% of organizations admit mobile devices are difficult to secure[8], it is clear that the convenience factor that mobile devices provide also raises the data security risks. And the rise of enterprise data access on mobile endpoints far outside legacy security infrastructure has left these attack surfaces ripe for phishing exploitation, leaving corporate and personal data at risk.

The fact remains that cybercriminals find mobile users particularly enticing for phishing attacks due to the lack of security surrounding consumer communication applications.

And according to Verizon's annual data breach report[9], this is due to mobile technology being an often-overlooked attack surface, opening the endpoint devices up to phishing attacks in ways that traditional desktop technologies do not.

[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] Department of Defense. Norton: Secure, operate, and defend are the fundamentals.
https://www.disa.mil/NewsandEvents/2017/AFCEA-Luncheon

[4] 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

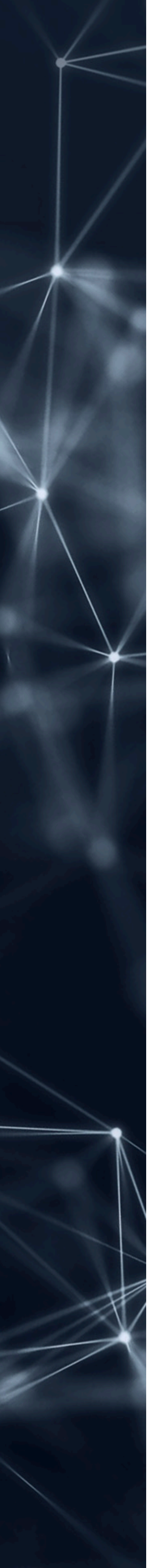
[5] Verizon. 2019 Data Breach Investigations Report. May 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[6] BYOD Usage in the Enterprise. https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf

[7] BYOTop 10 Email Clients in March 2019. https://uplandsoftware.com/adestra/resources/blog/top-10-email-clients/

[8] Enforce Endpoint Compliance and Cyber Hygiene With Duo Device Trust. https://blogs.cisco.com/security/enforce-endpoint-compliance-and-cyber-hygiene-with-duo-device-trust

[9] Ibid.



> "Attacks that proved successful on PCs are now being tested on unwitting mobile device users to see what works – and with the number of mobile devices with poor protection soaring, there are plenty of easy targets."
>
> - Stacy Collett, CSO Online

TOP 5 REASONS MOBILE TECHNOLOGY IS PHISHING-FRIENDLY

1 Users are in Charge

Mobile endpoint users typically administer their own devices, which lack the automated patching and updating policies found on enterprise desktops and laptops.

2 Less Usable Screen Space

The small screen size makes it more challenging to see the full web addresses on a browser and actual sender email addresses in emails.

3 Too Much Trust

Users feel a personal connection to their mobile devices that fosters unfounded trust in the device and the stored data and content.

4 Don't Ask, Just Tell

ACCEPT

GUI design encourages actions such as accept, reply, send, and like with limited information.

5 Texting While Distracted

The use of mobile devices while walking, talking, driving, and more mean users also respond to requests while distracted. By removing the need to view the originating app, mobile endpoint users are more likely to engage with the alert blindly.

Zimperium zIPS Protects Against Zero-day and Customized, Tailored Phishing Attacks

While security education is often considered the first line of defense against mobile phishing, it alone is not enough to stand up against the onslaught of phishing attempts plaguing enterprises. Ultimately, phishing attacks are more sophisticated and harder to detect even with the best end-user education. For enterprises to protect their data and endpoint users, they need to approach mobile device security with a combination of security layers.

Built on the patented z9 engine, Zimperium's machine learning engine is the security foundation of Zimperium zIPS, providing mobile endpoint phishing detection and zero-day attack prevention that legacy solutions often miss. And machine learning-based detection and prevention occurs on-device, without the need for network access, protecting users from previously unknown phishing attempts and increasing their mobile device security confidence. Shoring up the Zimperium z9 machine learning engine is a static analysis layer, increasing mobile phishing detection and prevention speed and efficacy.

With the z9 engine, zIPS can **detect both known and unknown threats** by analyzing slight deviations to a mobile device’s OS statistics, memory, CPU and other system parameters.

Cybercriminals are Phishing for Something

- Mobile Phishing increased more than 300% in 2020
- 32% of Confirmed Data Breaches Involved Phishing
- 37.9% of Users Fail Phishing Tests
- A New Phishing Site Launches Every 20 Seconds
- Department of Defense reported receiving 34 million malware-infested emails a day
- 78% of cyber-espionage incidents involved phishing

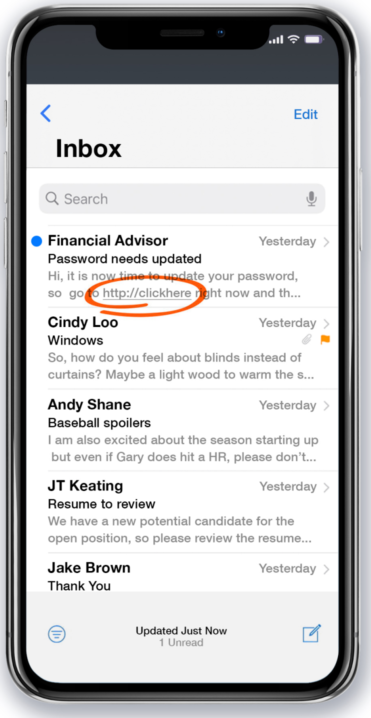
Zimperium zIPS provides robust and scalable mobile phishing protection, protecting mobile endpoints against this common data infiltration tactic. zIPS checks all links, whether email, text, social media or messaging app, determining if the link and source are legitimate and safe for the user to click. zIPS focuses on the mobile endpoint itself, providing full security coverage of both consumer and enterprise applications while raising security confidence.

Intuitive and easy to understand, zIPS mobile endpoint protection alerts the endpoint user if a URL is malicious before the connection being completed through simple and contextual alerts, helping users build better mobile security habits. And Zimperium zIPS provides this security layer without reading or parsing the messages' data, keeping personal data secure and private.

Falling within level 2 of Zimperium's Mobile Threat Defense (MTD) Maturity Model, mobile phishing protection is a proactive step for any organization looking to raise their mobile security confidence while enabling their employees to access and engage with corporate data from mobile devices.

Raise the Security Confidence with Advanced Mobile Phishing Protection

Due to the rise in mobile device use for enterprise data access and the almost unison increase in phishing attacks, the average organization's attack surface remains at risk until security controls are in place on all devices.



Financial Advisor Yesterday
Password needs updated
Hi, it is now time to update your password, so go to http://clickhere right now and th...

Cindy Loo Yesterday
Windows
So, how do you feel about blinds instead of curtains? Maybe a light wood to warm the s...

Andy Shane Yesterday
Baseball spoilers
I am also excited about the season starting up but even if Gary does hit a HR, please don't...

JT Keating Yesterday
Resume to review
We have a new potential candidate for the open position, so please review the resume...

Jake Brown Yesterday
Thank You

Updated Just Now
1 Unread

- 25% of phishing emails bypass legacy, default email client security

- Phishing URLs were presented to users via **three** separate, targeted social engineering campaigns.

- On average, targeted mobile endpoint users fall victim to **2** phishing links per month

It is time to treat mobile endpoints with the same security mindset as traditional endpoints and increase enterprise security confidence through advanced machine learning security mobile device security. Zimperium customers stand protected against even the most advanced and unknown phishing attacks.

- With an active Zimperium zIPS mobile phishing solution, enterprises saw more than **95%** decrease in successful phishing attacks.

- Gain **visibility** into **all phishing attempts** on all actively monitored mobile endpoints

- Zimperium's Security Score enables SOCs to understand overall risk posture and complement capabilities with end-user awareness training.

> "Zimperium's holistic approach to detection of phishing attacks targeted at users' mobile devices allows it to block phishing attacks that use text, social media, and personal and corporate email as vectors. It can do this while ensuring user privacy."
>
> - GigaOm's 2020 Radar for Phishing Prevention and Detection

Summary

Mobile phishing is top of mind for public and private sector IT security professionals and continues to be used as a vector of attack against enterprises of all sizes. Defending mobile users and their devices against phishing attacks needs to continue to be a top priority, combining both advanced technologies with user security training. 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 ready to help.

ZIMPERIUM®