Mitigating Mobile Phishing Threats with Zimperium Mobile Threat Defense (MTD)

MTD™

ZIMPERIUM®

What is Phishing?

At its most basic level, the term phishing describes an attacker's attempt to trick a person into revealing sensitive information. In recent years, here's how the process would typically work:

- First, cybercriminals would create a web page that mimics the site of a recognized business.
- Then the attacker sends emails purporting to be from that established business, hoping to lure users to the web page.
- Finally, when a user submits their credentials on the compromised page, the attacker retrieves those credentials and uses them to gain access and pursue their nefarious objectives.

According to recent research, 68% of breaches involved the human element, and phishing is by far the most common form of social engineering tactic, accounting for more than 60% of these attacks.[1] In 2023, 76% of organizations experienced an email-based phishing attack that successfully tricked a user into taking a risky action, such as clicking a malicious link, downloading malware, submitting credentials, and even initiating a wire transfer.[2]

76%
of organizations experienced an email-based phishing attack

How is Phishing Evolving?

While the use of email and web pages remains a standard model, it seems each new day brings a new set of tactics. Email and malicious web pages are only the proverbial tip of the iceberg in terms of the tools phishers may use. Now, an adversary may wage their attacks via a number of different channels, including voicemails, instant messaging, Zoom chats, and messages sent via such apps as LinkedIn, Microsoft Teams, Google Meet, WhatsApp, and more.

Attackers may use multiple channels to wage a single attack, whether to evade defenses or make their communications appear more credible more effectively. For example, an attacker may use a WhatsApp message to send what seems to be a Microsoft Teams meeting invite. When clicking on the invite link, victims are directed to a malicious landing page that asks them to provide their Office 365 credentials.

Why Does Mobile Phishing Represent Such an Urgent Threat?

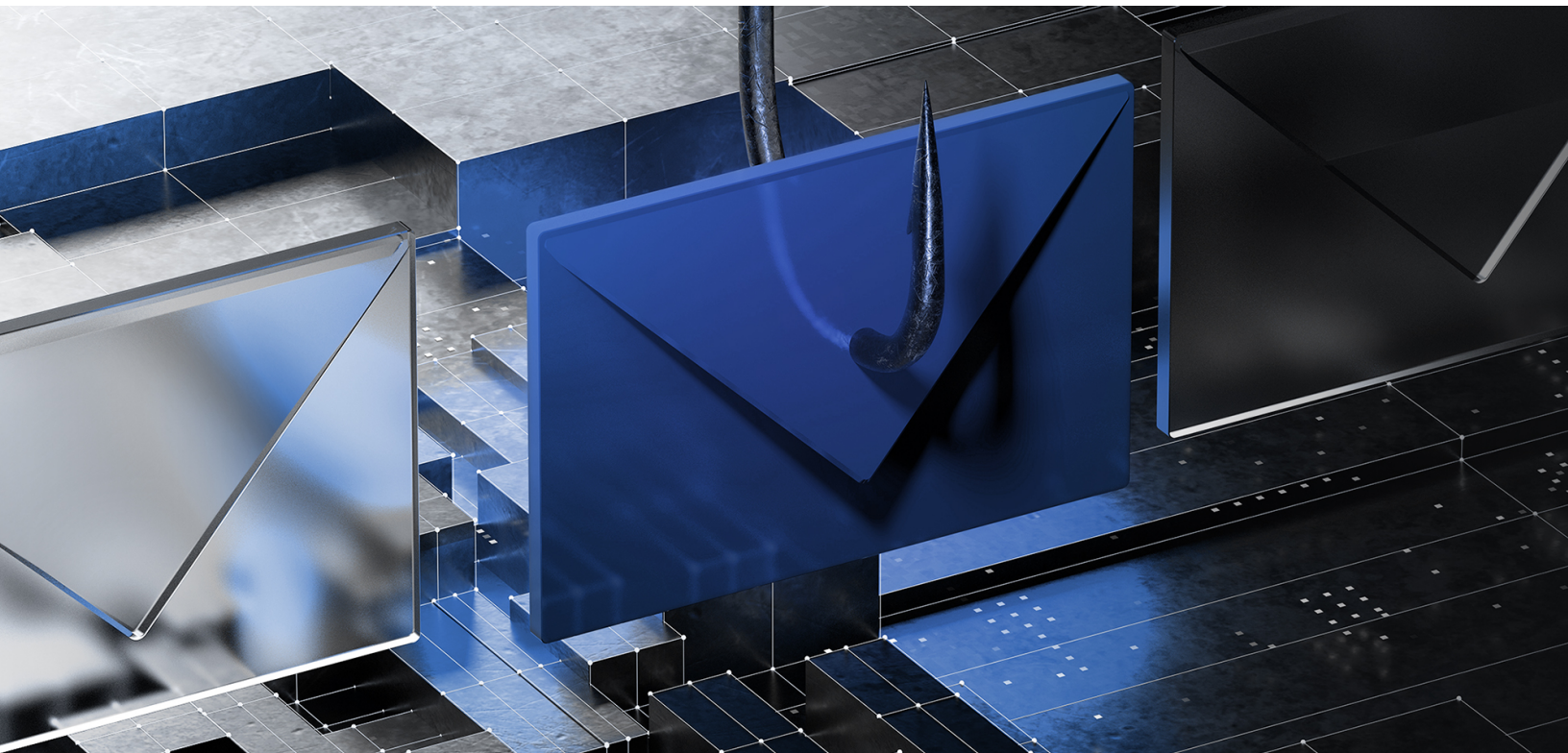
The use of phishing that targets mobile devices continues to grow more common and presents an increasingly urgent threat to enterprises and government agencies. That's because:

- **Mobile devices are more relied upon.** Today, mobile devices are an increasingly integral part of our professional lives. As remote and hybrid work continue to grow more commonplace, so does the use of mobile devices to stay connected and get work done. Whether in a corporate office, at a café, or on a plane, employees are increasingly using their mobile devices to access corporate cloud-based and on-premise-based services. In one report, 53% of respondents said mobile devices have access to more sensitive data than the prior year. [3]
- **Mobile devices are more interconnected.** Given an employee may reuse credentials across multiple apps and services, one successful phishing attack may expose many other services.
- **Mobile devices are more vulnerable.** In most enterprises, mobile devices do not have the same protections as traditional endpoints like laptops. For enterprise security teams, this makes it far more difficult to detect active threats, especially in a bring your own devices (BYOD) scenario. Further, with mobile devices' smaller screens, it can be more difficult for users to detect the common red flags associated with phishing.

Given all these factors, phishing attacks targeting mobile devices are not only increasingly common, but they're also increasingly successful. According to one report, almost one-fifth of phishing successes come from mobile devices[4]. Plus, the reality is that—given the limited visibility many security teams have on mobile devices—the numbers may be much higher. Another report found that 51% have experienced mobile application related incidents from factors such as malware or unpatched vulnerabilities. [5]

Mobile Phishing May Just Be the Beginning

In many cases, phishing is just the initial step of a much larger operation. Once a phishing attack successfully acquires an end user's credentials or installs malware, the device, the user, and, by extension, the company may be vulnerable to a range of subsequent threats. Quite often, the ultimate prize for cybercriminals is a ransomware attack that targets an enterprise or government agency, which can yield the biggest payday. Specifically, phishing emails were the leading point of entry for ransomware, constituting around 54% of those attacks. In fact, 75% of ransomware incidents involved the use of desktop sharing software (45%) and phishing email (35%)[6].These phishing emails distribute malicious links or attachments that attackers ultimately use to gain access to systems, so they can encrypt an organization's assets, disrupt operations, and make ransom demands.



Which Industries Are Being Targeted by Mobile Phishing and Ransomware?

Given these realities, it's no surprise that government agencies and large enterprises in healthcare, financial services, and manufacturing are routinely targeted. Following is more information on how mobile phishing and ransomware are hitting each of these industries:

Healthcare

Nearly 66% of healthcare organizations experienced a ransomware attack in 2021. In the prior year, over 600 hospitals, clinics, and healthcare organizations were impacted by 92 ransomware attacks, affecting operations, patient data, intellectual property, and potential health integrity of patient care.[7]

Financial

In 2021, phishing was the most common threat vector for financial services, making up 14% of all attacks, while 70% of those attacks were on banks.[8]

Manufacturing

It is estimated that the manufacturing sector accounts for 23% of ransomware reports. The highest average ransomware payments in manufacturing reach nearly $2.04 million.[9]

Government

In 2020, 79 ransomware exploits on local government agencies have resulted in disrupted operational services, the risk to public safety, and financial losses. The public's dependency on critical utilities, emergency services, educational facilities, and other services makes them an attractive target for adversaries.[10]

How Zimperium MTD Can Help

Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - is an advanced mobile threat defense solution for enterprises, providing persistent, on-device protection to Android, iOS, and ChromeOS. In addition, Zimperium's mobile threat defense engine adds advanced mobile phishing detection using a combination of traditional security and state-of-the-art known and zero-day threat detection from a wide range of attack vectors.

- **Threat Research:** Phishing protection is achieved by extensively monitoring known phishing sites and extracting hundreds of features to fingerprint and classify zero-day phishing sites.
- **Phishing Classifiers:** Detects traffic from the malicious domains with our machine learning-based technology, blocking all traffic and preventing attackers from redirecting a potential victim to a targeted phishing site.
- **Offline Phishing Detection:** Zimperium's mobile threat defense provides always-on detection and protection against threats even when external servers are out of reach.
- **Content Filtering:** Safari Browser Extension and web content filtering relies on Zimperium's web content filtering engine to detect 10x more categories than our competitors.
- **QR Code Scanning:** Protects end-users from QR code phishing attacks before they become a threat to the device.
- **SMS Phishing Detection:** Scans URLs on Android and iOS iMessage for phishing threats.
- **Scalable Integrations:** Incident Response teams finally have visibility into mobile threats and risks through integrations with leading UEM, SIEM, SOAR, and XDR systems. The unmatched forensics provided by MTD prevent a compromised device from becoming an outbreak by rapidly identifying key IoCs, risk indicators, and vulnerable devices.

Zimperium is the only pure-play Mobile Threat Defense provider recognized in GiaOm's Anti-Phishing Radar Report.

To learn more about how Zimperium helps mitigate phishing threats to your business on BYOD and managed devices, contact us today at www.zimperium.com/contact-us/

Sources

1 Verizon, "2024 Data Breach Investigations Report," https://www.verizon.com/business/resources/T8c9/reports/2024-dbir-data-breach-investigations-report.pdf

2 Proofpoint, "2024 State of the Phish," https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf

3 Verizon, "Mobile Security Index 2024," https://www.verizon.com/business/resources/T6ea/reports/2024-mobile-security-index.pdf

4 Verizon, "2022 Data Breach Investigations Report," https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

5 Verizon, "Mobile Security Index 2024," https://www.verizon.com/business/resources/T6ea/reports/2024-mobile-security-index.pdf

6 Verizon, "2022 Data Breach Investigations Report," https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

7 HIPAA Journal, "'Healthcare Ransomware Attacks Increased by 94% in 2021," https://www.hipaajournal.com/healthcare-ransomware-attacks-increased-by-94-in-2021

8 IBM, "X-Force Threat Intelligence Index 2022," https://www.ibm.com/security/data-breach/threat-intelligence/

9 Cybersecurity Dive, "Ransomware attacks, payouts soared worldwide in 2021: report," https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/

10 Camparitech, "Ransomware attacks on US government organizations cost $18.9bn in 2020," https://www.comparitech.com/blog/information-security/government-ransomware-attacks/