WHITEPAPER

Mobile Phishing

corrata

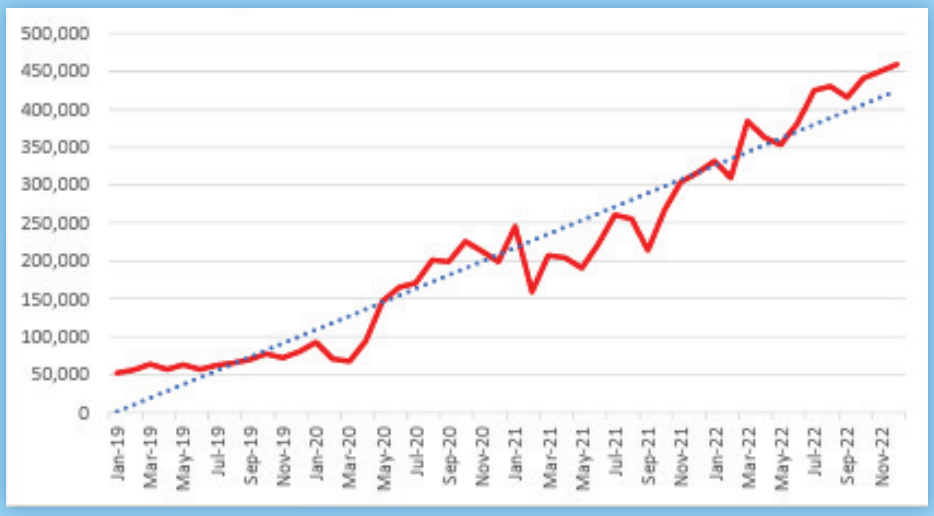
Introduction

Phishing is a deceptively simple, yet potent, form of cyberattack. In its 2021 Cyber Threat Trends report, Cisco highlighted that 90% of data breaches involved phishing. Despite the constant warnings about phishing and longstanding awareness of these attacks, they continue to pose a significant threat.

Cybersecurity teams have been tirelessly combating these attacks and, today, all email services include spam and phishing filters. Despite the constant enhancements in phishing defense technology, some phishing attacks still manage to succeed in penetrating these defenses.

The persistent threat of phishing can be attributed to cyberattackers' adaptability and relentless efforts to escalate their tactics in the ongoing cybersecurity arms race. Recent advancements, such as the employment of encrypted websites for hosting phishing, and the utilization of phishing toolkits, have amplified the efficacy of phishing attacks. These toolkits have made mobilizing phishing attacks exceptionally easy. The latest development in this field are toolkits that employ proxy architecture to circumvent multi-factor authentication. What's more, the rapid pace of attacks and short lifespan of many phishing sites have made it challenging to keep threat intelligence feeds updated, making defense even harder.

Phishing Attacks, Jan 2019 to Dec 2022



Source: *Anti-Phishing Working Group.*

The amplified threat of phishing isn't solely due to attackers' increased technical sophistication. The potential damage from credential theft has been dramatically heightened by the shift to cloud computing and Software as a Service (SaaS). Unlike in the past, when physical access to a network was often necessary to access certain applications, now all one needs is an internet connection and the credentials of an authorized user.

This paper focuses on the threat posed by a specific category of phishing attack: those targeting mobile devices. While phishing is traditionally associated with email, 85% of attacks on mobile devices come through channels such as SMS, WhatsApp and other messaging, social media, and collaboration applications. Any channel that can display a clickable link to a user is a potential delivery platform for a phishing attack. It's important to note that links delivered to your phone are seldom vetted. At least with email applications, there's some degree of protection due to email filtering, but such technology is rarely used to screen other channels on mobile devices.

The other fact is that users are more prone to click on links they view on their mobiles devices than on their laptops. Factors including limited screen space, fewer visual cues, and the way we consume content on the move, significantly increase the likelihood of falling prey to a well-executed phishing scam. When you're sitting at your desk in front of a computer in "work mode", you tend to be more vigilant. But the same can't be said as you stand waiting at the bus stop after a night out scrolling through your phone(!)

How would you like your phishing delivered today?

Consider all the ways in which a phishing link could appear on your phone. You could receive a malicious email that bypassed your email filtering service, or an urgent SMS from your HR department asking you to update your employee record. You could receive a link innocently forwarded by a friend in a WhatsApp message or be targeted while interacting with a chatbot or scanning a QR code.

All these channels have been used successfully to steal business application credentials. Uber and Twilio are two well-known companies that suffered breaches starting with SMS phishing (smishing) messages. In the case of Twilio, the attack began with an SMS which was sent to 88 employees asking them to urgently log in to their support ticketing system. A significant number of employees not only clicked the link, but also entered their credentials. This gave the attackers a foothold in the company's systems, which they then exploited to exfiltrate significant amounts of sensitive data.

Examples of SMS phishing messages used in Twilio breach

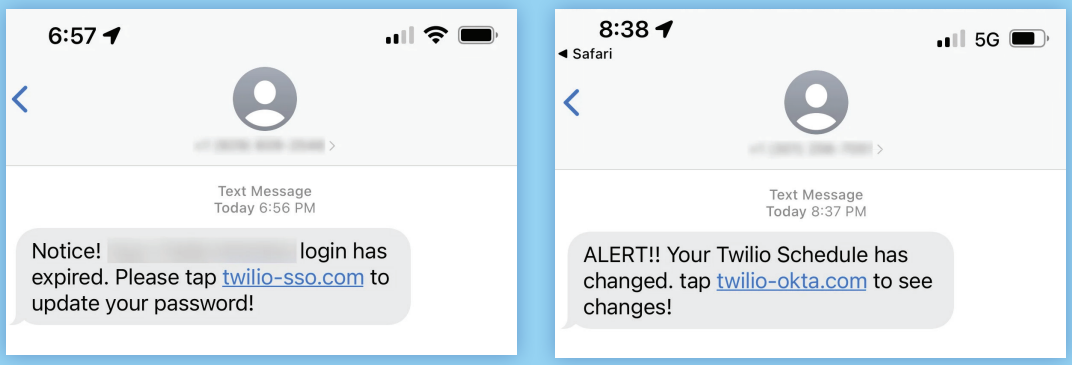
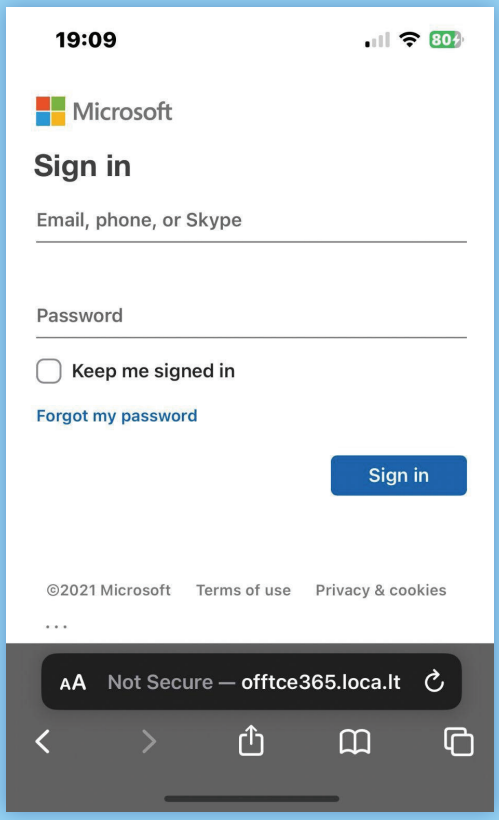


Image source: Twilio.com

Phishing attacks extend beyond coaxing users to reveal their login credentials. They can also involve deceptive tactics to entice users into downloading harmful applications. It's surprisingly simple to convince employees to install unauthorized apps. When an organization first deploys Corrata's mobile security solution, we often discover that 5% or more of employees have sourced apps from unverified third-party stores or insecure websites. The lure typically hinges on the potential to access content or features usually not freely available, such as the latest episodes of a popular TV series or a newly launched game. Once installed employees are duped into granting the app access to sensitive functionalities, like sending and receiving messages (which could be exploited to capture multi-factor authentication codes), or reading and rewriting screen content (which could be used to intercept communications). Cybercriminals can exploit these "dangerous permissions" to steal login credentials, intercept two-factor authentication codes, and eavesdrop on communication content.

Example of fake Microsoft365 login page



Vulnerable employees and zero protection.

The threat of mobile phishing isn't solely due to the multiple channels cybercriminals can exploit. Its danger is amplified because mobile phishing attacks are difficult to spot; users are less vigilant and mobile devices rarely have the extensive cybersecurity defenses that are present on laptops and desktop computers.

Recognizing a mobile phishing attack is tricky due in part to the smaller screen size and the less detailed browser interfaces, compared to those on desktops. But even more significant is the casual attitude towards mobile use. Mobile devices blur the line between work and personal life. One minute, you're making social plans. The next, you're handling sensitive work matters. This fluidity often leads to a lapse in the caution that typically accompanies desktop usage.

Historically, security professionals have associated phishing primarily with email and, even today, it remains a prevalent method for phishing attacks on desktops and laptops. Email services like Microsoft Outlook and Gmail have integrated anti-spam and anti-phishing measures, and many organizations supplement these with additional solutions from providers such as Proofpoint. While not foolproof, these defenses are crucial, especially when combined with employee training, multi-factor authentication, and web filtering.

However, mobile phishing presents a different type of challenge. 85% of it occurs outside email, commonly via SMS, which lacks in-built anti-phishing measures. Some telecommunications providers use SMS firewalls to filter malicious content, but their

implementation is inconsistent and their effectiveness patchy. These providers also lack the robust threat intelligence sharing mechanisms offered by organizations like the Anti-Phishing Working Group.

Attempts by Google and Apple to implement device-level protections (within the messaging client) are hindered by privacy concerns. Most users don't like the idea of "big tech" reading their messages. Browser protections, such as those in Chrome and Safari, do provide some assistance but, due to their mass-market design, they often respond too slowly to new threats. In a recent test, for instance, Chrome blocked fewer than 17% of new smishing attacks.

The coverage of web filtering solutions, another common technology deployed to block malicious links, rarely extends to mobile. This disparity is yet another manifestation of the security gap existing between traditional endpoints and mobile devices.

It's also worth noting that mobile device management (MDM) systems like Intune or Workspace ONE don't offer protection against phishing or other cyber threats like malware or spyware.

The bottom line is that, when it comes to mobile phishing, organizations are alarmingly vulnerable. In the age of cloud computing, this level of risk is simply unacceptable.

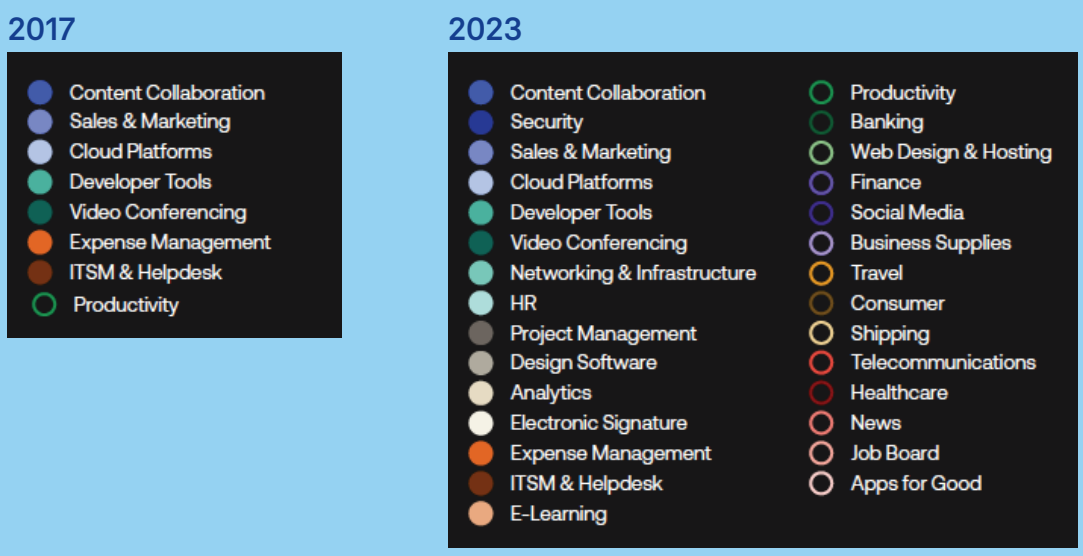
Mobile phishing in the cloud computing era.

The smartphone has transformed the world in which we work. Being able to access email on the move was a game changer but, in the last few years, many other business applications have been mobile-enabled and, in some cases, completely re-engineered to take advantage of the productivity gains afforded by "do anywhere" capabilities.

However, nothing has prepared us for the new reality of the cloud era. Mobile phones now have, in many cases, the same level of access to corporate data as a laptop or desktop computer connected to the corporate network. Applications for sales, finance, logistics, manufacturing, human resources, and much, much more, are now all delivered on a SaaS basis with mobile access which is on a par with desktop.

But our security approach hasn't evolved sufficiently to recognize this reality. Partly, this is inertia and lack of awareness and, partly, it's a false sense that exposure is limited because employees don't routinely use every application available to them on their mobile.
This couldn't be further from the truth. Your employee's mobile phone now has access to the vast majority of the data your organization not only cares about but is legally responsible for.

Growth in categories of SaaS apps 2017 to 2023



Because enterprise applications are now routinely accessible anywhere, the level of reliance placed on identity has gone through the metaphorical roof. Effectively, if an attacker can steal credentials and bypass multi-factor authentication, they have the keys to your kingdom. Combined with ubiquitous mobile access, we have turbocharged the risk your employees face on mobile. A phishing link targeting a mobile user can now ask for credentials to almost every system in your organization. With these credentials to hand, the attacker can now access that critical system from almost anywhere. Even when you've implemented multi-factor authentication (MFA), the attacker can access that system using MFA bypass techniques. A combination of anywhere, anytime access and the rich phishing opportunities that mobile presents changes the equation for mobile endpoint security. It can no longer remain a poor relation.

Security professionals are well aware of how regularly user credentials are stolen. Because of this, the industry has rightly promoted the adoption of MFA. MFA addresses the risk of account compromise by ensuring that possession of a username/password combination alone is no longer enough to get access. Now the attacker must also be able to get hold of a second factor. This can take many forms: a one-time use code sent to a trusted device, a code generated by an authenticator app, an authentication device, or a biometric identifier. But introducing MFA is not without its challenges. Employees and customers need to be educated in the new process and often view the additional security step, or steps, as an annoyance. Nonetheless, there has been real progress, and a variety of industry surveys suggest that, today, more than 50% of organizations have implemented MFA.

But in the arms race that characterizes the battle between cybersecurity attackers and defenders, the bad guys have responded with new techniques which have been successful in breaching accounts protected with MFA.

They have achieved this by combining phishing with a variety of other methods. These

include re-directing one-time use passwords sent over SMS to a cloned SIM card (SIM swapping) or using mobile malware to capture authentication codes. Generating repeated authentication requests against an account can lead a user to approve access to stop the incoming requests; a technique dubbed "MFA fatigue". But, by far, the most dangerous technique for undermining the effectiveness of MFA is an attack which combines phishing with a method known as "Adversary-in-the-Middle" (AiTM). Rather than intercepting the one-time password, this technique works by "listening in" on the login process and then stealing the authentication cookie generated when a user logs in successfully.

As in all phishing attacks, an AiTM attack starts with a malicious link delivered over email, SMS, or some other messaging platform. But instead of re-directing to a fake login page, the link sends the user to a server which transparently forwards the user's request to the legitimate site. This "reverse proxy" simply sits in the middle and is invisible to the end user. Once the user successfully authenticates, by entering their password and one-time use code, the attacker steals the authentication cookie.

Once in possession of the cookie, the attacker can inject this into their browser and have unrestricted access to the compromised account without the need to provide a username, password, or second-factor code.

Transport layer security is a fundamental building block of security on the web. It ensures that, even when they can intercept communications, attackers have no way of decoding their contents.

However, encryption doesn't protect against an AiTM attack. The user who falls for the lure and clicks on the malicious link believes they are requesting to connect to a legitimate site. An encrypted session is created between the user's browser and the site to which it connects (so you'll see the lock sign in your browser). But everything you enter, including your username, password, and authentication code, is fully visible to the attacker, as it is their website to which you are connected. The attacker then logs into the legitimate site (for example, Microsoft365.com) on your behalf. You now have access to the service as expected, but so does the attacker, who has, unknown to you, copied your authentication cookie. With the authentication cookie, the attacker is free to log in into the compromised account for weeks, or even months, after the initial breach.

To make matters worse, potential attackers now have access to a range of toolkits, including Greatness, Modlishka, Necrobrowser, Evilginx2, and EvilProxy, which are making it increasingly easy to launch this type of sophisticated attack.

Defenders Playbook

The good news is that help is at hand, with mature and effective anti-phishing solutions for mobile now available. A range of specialist mobile threat defense solution providers, of which Corrata is one, provide effective and easy-to-deploy smishing protection as part of their broader mobile threat defense products.

These solutions work at the device level by examining any link that a user clicks, whether embedded within a website, application, SMS, WhatsApp message, or other messaging app. If the link is dangerous, then access to the site is blocked, the user notified, and an alert sent to the security operations team.

Traditional endpoint security vendors (e.g., Microsoft Defender, CrowdStrike, SentinelOne, McAfee, Sophos, Trend Micro) also offer mobile versions of their desktop products. Many feature anti-phishing protection. A recent analysis by Corrata security researchers has shown that these "suite solutions" perform poorly at detecting and blocking smishing and other types of mobile-specific phishing attacks.

Our researchers took a sample of recent SMS phishing attacks and examined how many were blocked by mobile threat defense solutions provided by the "traditional" vendors and compared it with the percentage blocked by Corrata. The results were clear-cut. The traditional suite solutions (provided by household names in enterprise tech) caught

only 39% of the smishing attacks. In contrast, the Corrata solution captured 100% of the malicious messages.

While we weren't surprised by how well our solution performed, we were quite taken aback at how poorly the suite vendors performed. Our hunch is that they lack the right threat intelligence and mobile specific detection techniques - they are relying on threat feeds, which are built to defend against the threats they see every day on desktop, in email, etc. By contrast, the Corrata threat feed is "mobile first", incorporating traditional threat feeds but augmented with mobile-specific threat intelligence. But Corrata goes further. We fine-tune our algorithms to detect new threats even before they've been identified by the broader threat intelligence ecosystem, and we work closely with a range of partners to make sure we are always one step ahead.

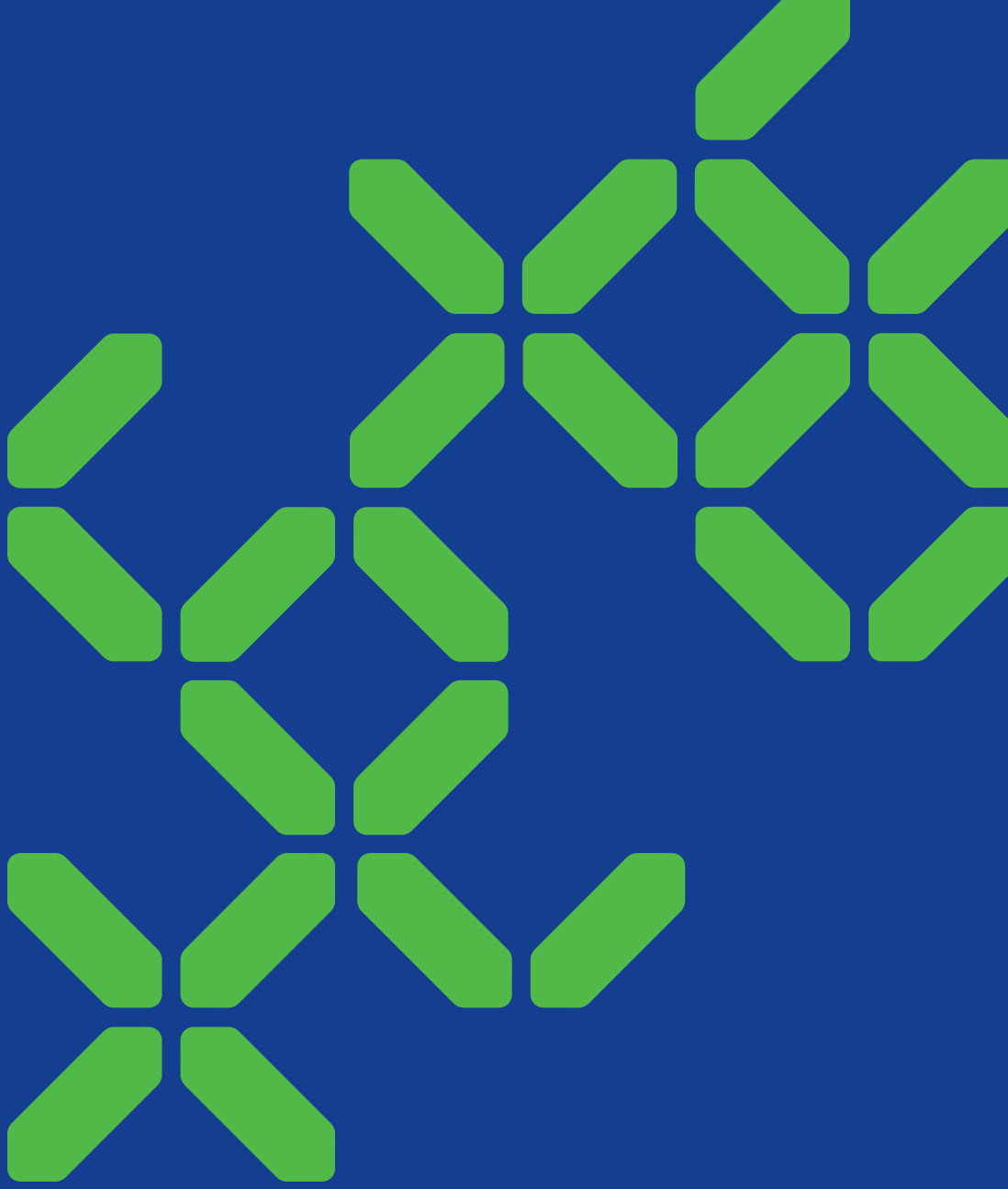
Reliable, up-to-the-minute threat intelligence is critical in defeating phishing and other cyber threats. SMS phishing, in particular, is a very fast-moving game with new attacks launched and taken down in hours, if not minutes. This means that adopting the precautionary principle is often the only correct approach. But this must be done in a subtly calibrated manner to avoid impacting the experience and productivity of staff.

Conclusion

Mobile phishing is a real, distinct threat which organizations are only now beginning to fully understand. On a mobile device, attackers have a wide range of alternative channels to deliver phishing links. The protections in place to counter traditional phishing on laptop and desktop computers are completely absent on mobile. Employees are less vigilant when using mobile phones, and smaller screen sizes make it harder to detect phishing messages.

While all of this has been true for a long time, what has changed in recent times is that, today, with the acceleration to cloud and remote working, employees can now access most, or all, of their employer's critical business applications (previously only accessible with a network-connected laptop or desktop) on their mobile device.

What has also changed is that attackers have upped the velocity and sophistication of their attacks on mobile. They have recognized the opportunity. Defenders, and businesses just like yours, must now recognize, understand and respond.



corrata

corrata.com