



Mobile Phishing:

*From email to social media –
the latest security threat facing
enterprise mobility*

Table of Contents

| | |
|----------------------------------|----|
| Introduction | 3 |
| What is Phishing? | 4 |
| Why Mobile? | 5 |
| Types of Phishing Attack | 6 |
| - Email | 6 |
| - SMS | 7 |
| - WhatsApp | 8 |
| - Malicious Apps | 9 |
| - Social Media | 10 |
| Corrata Mobile Security Solution | 12 |

Introduction

Mobile devices, such as smartphones and tablets, have become essential to our everyday lives both at work and at home. The use of mobile devices has extended in particular to the full range of digital workplace tools including email, calendaring and file sharing. This has allowed employees more convenience and flexibility when completing work related tasks resulting in greater innovation and productivity.

Mobile phishing attempts
grew by

65%

in 2017

- *PhishMe*¹

Smartphones and tablets
now account for over

60%

of all smart connected consumer
devices - up from 17% in 2008

- *IHS Markit*²

However with this increased use of mobile, new avenues for cyberattacks have emerged. In particular, new types of phishing attacks, for years generally thought to be restricted to email, have emerged in response to the rapid increase in mobile usage. Cybercriminals have recognised the potential value in exploiting channels such as social media, messaging services and mobile apps, to steal information from users. As mobile devices generally lack the security measures afforded to desktops and as the lines between personal and corporate devices blur, mobile creates an ideal opportunity for phishers and exposes organizations to risk of fraud and data loss.

But what exactly is mobile phishing and how might your organization fall victim to such attacks? Why have mobile devices become such attractive targets for cybercriminals? And what can organizations do to protect themselves from such attacks?

¹ PhishMe, *Enterprise Phishing Susceptibility and Defense Report 2017*

² IHS Markit, *More than Six Billion Smartphones by 2020, HIS Markit Says, 2017*

What is Phishing?

Phishing is an extremely simple yet effective method of cyberattack. In 2017, Verizon reported that phishing was involved in 95% of reported security breaches. Let's look at what is involved in common phishing attacks and how they can open up organizations to threats including data loss and fraud.



95%

of reported security breaches in 2017 involved phishing

- Verizon³

Another common trait of phishing messages involves sending the user a hyperlink to another website or an attachment to download, both of which seem legitimate and can often be identical to the original source they are trying to imitate. These websites however will then be used to collect the user's personal information, while the attachments will contain ransomware or other viruses that can infect the device.

Phishing attacks involve directly contacting a user and posing as a legitimate person or institution in order to steal sensitive information, including contact and financial details and online login credentials. This information can then be used to access important online accounts and can result in data or financial loss. Commonly, phishing messages contain urgent or eye-catching statements and offers that grab the user's attention and encourage them to act quickly. However these offers can often seem too good to be true for a reason – they usually are.

Spear phishing is a more targeted campaign that attacks a specific individual, organization or business by personalizing the communication and posing as a trusted source to lure the victim into a false sense of security. E-mail has generally been the main channel used for phishing attacks however in recent years, platforms such as SMS, WhatsApp, social media sites such as Facebook and Twitter, and mobile apps have become popular among cybercriminals, especially as the use of mobile devices continues to increase.

³ Verizon, Data Breach Investigations Report 2018

Why Mobile?

Phishing is a great example of how mobile opens up gaps in the traditional cyber security architecture. Typically there are two layers of protection against phishing attacks for email. In the first instance, there is a mail filter which blocks suspicious emails before they are delivered to the employee. A second layer of protection is then offered by the corporate web gateway which will scan and block access to malicious links contained in the email in real-time, in the case of a suspicious link making it through the initial filter.

The first security gap emerges where the phishing message is received on mobile. When outside of the corporate network, mobile devices are not protected by the company's secure web gateway (SWG) and do not have the protections it provides. Without real-time threat surveillance and scanning, employees will not be restricted from accessing malicious links and with more and more employees using mobile to access corporate email and communications both inside and outside the office, this makes the device especially vulnerable to attack.

The second security gap emerges where phishing attacks are executed over a medium other than email. For example, as SMS messages go nowhere near the mail server, a phishing SMS will not be stopped by the mail filter and there will be nothing in place to stop an employee from clicking on a malicious link. Similarly links can be distributed over messaging services like WhatsApp, and social media platforms like Twitter and Facebook, which as the device is not protected by the web gateway, can trick employees into revealing login credentials, installing rogue profiles on iOS or downloading malware to Android devices.



"Mobile users are 3x more likely to fall for a phishing attack than desktop users"

- IBM⁴

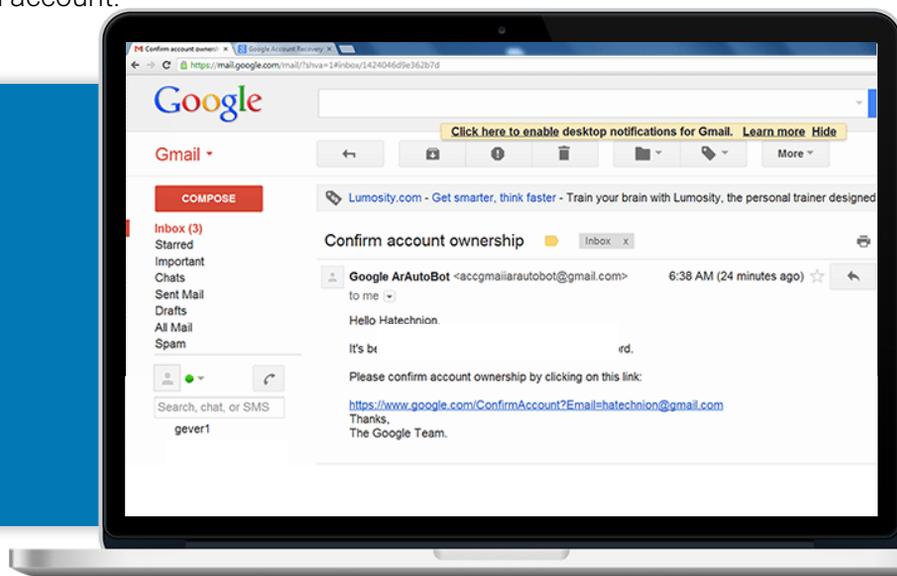
⁴ IBM, 'Mobile Users 3 Times More Vulnerable to Phishing Attacks', 2011

Types of Phishing Attack

Email

Most security professionals and individual users are aware of the prevalence and danger of email phishing. Typically these attacks take the form of emails from cybercriminals posing as trustworthy bodies and convincing the user to disclose their personal or financial details. For example, users have reported receiving an email appearing to be from Google that requires them to follow a hyperlink and input their username and password in order to verify their Gmail account. However this then turns out to be a phishing attack used to steal these credentials and gain access to the user's email account.

Phishing attacks are used to steal credentials and gain access to the user's email account.



These types of phishing attacks have existed for quite some time and as a result, enterprise email systems have seen heavy investment in anti-phishing technology. These solutions can detect and prevent phishing emails from reaching the employee's inbox, while navigation to any suspicious or malicious site is blocked by the corporate network's SWG. As well as this, employees are often well-educated to be suspicious of emails sent from unknown sources and to be vigilant of the information disclosed over email.

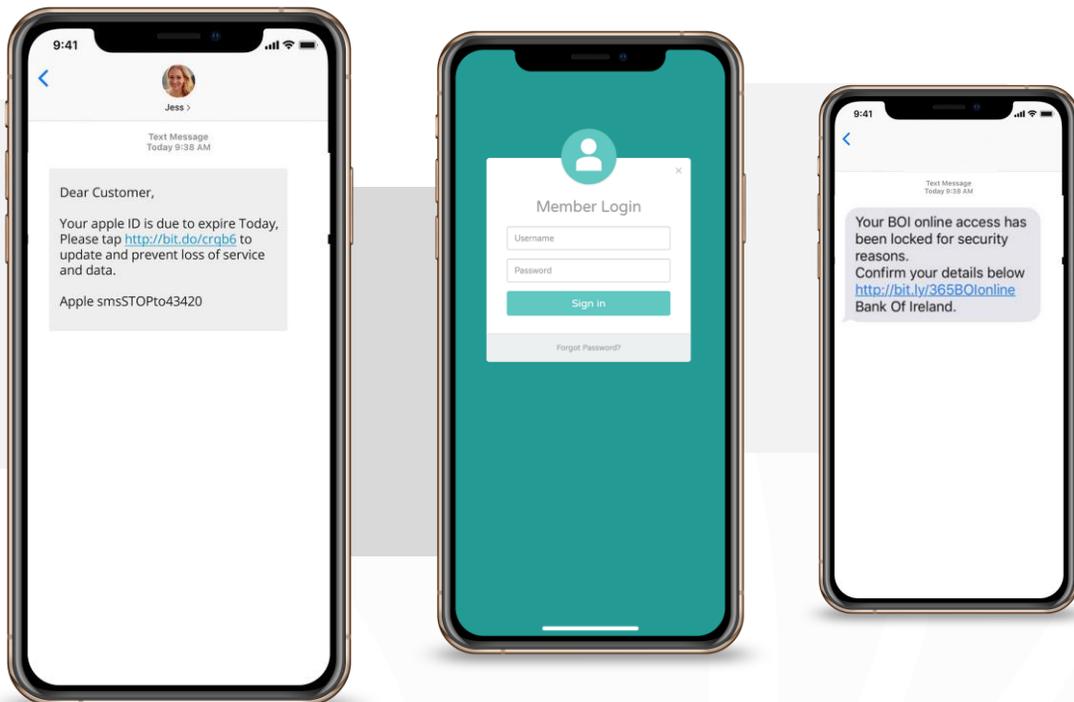
However with over 66% of emails⁵ opened on mobile devices, it still remains a popular tool for attempted cyberattacks. Often supported by the time delay in receiving and opening the email, malicious links on mobile cannot be scanned in real-time or be blocked by the SWG leaving employees vulnerable to attack.

⁵ MovableInk, 'US Customer Device Preference Report: 2015 Year in Review'

SMS

'Smishing' is a popular form of phishing as it focuses the attack on an often overlooked component of organizational cybersecurity: SMS text messaging.

- The attacker sends a text to the victim's phone that persuades them to click a link found in the message.
- Clicking this link results in one of two possibilities – the link loads a phishing page where the user is tricked into inputting their login credentials, or it initiates a silent download of surveillance spyware to the device.
- Ultimately, the attacker's aim is to gain unauthorized access to personal, sensitive and corporate data stored and accessed by the device.

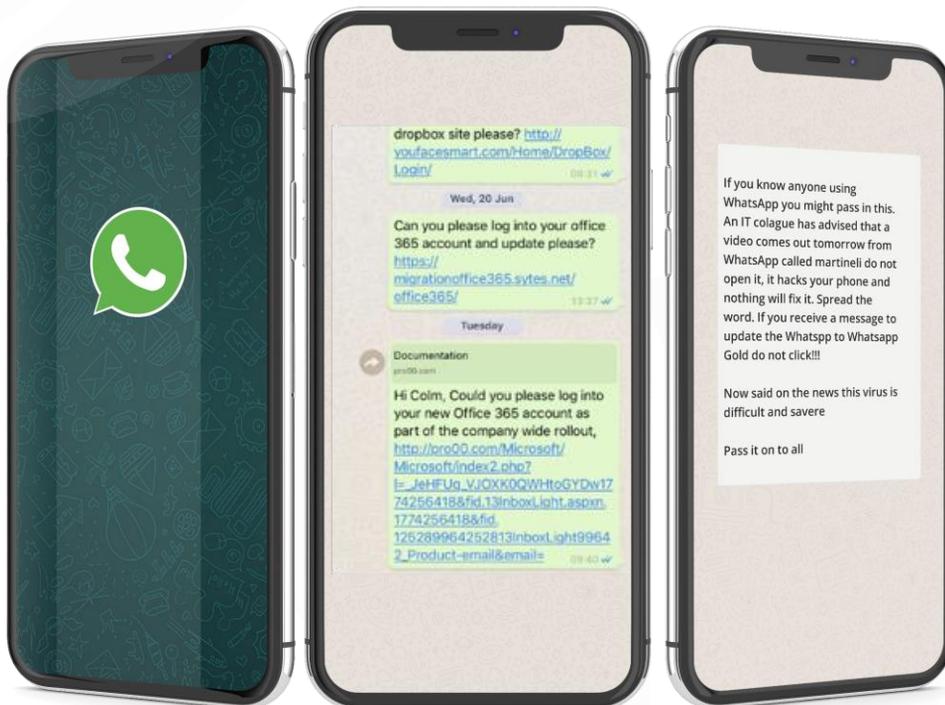


WhatsApp

'Whishing' is the term coined to describe WhatsApp phishing. WhatsApp enables communication with anyone else on the platform and therefore phishers can target a huge amount of users with the same blanket message.

WhatsApp is a cheap and relatively easy way to quickly reach lots of users, which is why 'whishing' is becoming prevalent. Again, the mechanics are as simple as clicking a malicious link in a WhatsApp message, but the consequences are anything but innocent.

WhatsApp-based phishing, like any phishing attack, can be neutralized by blocking connections to the phishing server using a web gateway. However, today's existing web gateways only work for devices when they are connected to the corporate network. Mobile devices by their very nature are designed to be used on any network and therefore they lack protection against phishing attacks.



Malicious apps

Applications downloaded onto the device can also be used in phishing attacks to install malware or defraud and steal sensitive information from the organization. There are several ways that malicious apps can end up on a mobile device. The first is from unofficial app stores. Users are directed from an internet search towards an unofficial app store and unknowingly download a mobile application not made by the original creators. Therein lies the risk of downloading malware and other mobile-specific viruses, because there is no enforceable guarantee that the download is the desired app. Another entry point for phishing attacks is through malicious apps on official app stores. There have been countless cases of removals from iOS and Android app.

Stores of apps that prompted downloads of malware or led users to click on links that demanded payment or solicited sensitive information. For example an attack reported earlier this year involved a fraudulent app downloaded from the official App Store. Once installed, the app would display an imitation dialog box, extremely similar to the official Apple dialog box, asking for the user's Apple ID and password. Entering these details is an extremely common occurrence when using Apple devices and therefore would not be a cause for concern for the employee but once the details were entered would grant the phishers access to their iCloud account, email, contacts, calendar and messages, resulting in major data breach issues.



There have been countless cases of app removals from iOS and Android app stores.

⁶ Infosecurity Magazine, 'Social Media Phishing Attacks Soar 500%', 2017

⁷ InformationSecurityBuzz, 'Phishing Via Social Media Up 100 Percent, Now a Preferred Vector', 2018

Social Media

Phishing attacks originating from social media soared by **500%⁶ in 2016, and by a further 100% in 2017⁷**. Social media is fast becoming an extremely popular method of attack for phishers, and while workplace desktops are likely to have enterprise-level security solutions installed, mobile devices are generally ignored. This leaves the user free to engage with potentially malicious content, as they please. The problem arises when they do inevitably engage with a malicious link embedded in a social media post. This is an extremely common way to trick unsuspecting users into revealing personal information and other sensitive credentials, such as those used to access corporate accounts or systems. Malicious links appear across many social media platforms, and not just for the most popular recreational sites such as Facebook, Twitter and Instagram. Even professional networking platform, LinkedIn, has been known to play host to similarly malicious phishing attempts. If these attacks are realized through a security-lacking mobile device, it puts both the user and organization at tremendous risk.

Facebook

Facebook phishing attacks often involve posing as a trusted friend in order to gain the users trust and lure them into clicking a malicious link or divulging personal information

LinkedIn

LinkedIn has become extremely popular for phishing attacks likely due to the assumption that all members are professionals looking to make connections therefore inciting trust amongst users

Twitter

Common Twitter phishing campaigns take advantage of customer-brand engagement and pose as legitimate accounts of well-known brands and companies

Instagram

Similarly to Facebook and Twitter, Instagram phishing attacks mostly focus on masquerading as legitimate friends or brands in order to fool users entering their account details on bogus login pages

Corrata's Mobile Security Statistics

19%

of social media accounts
appearing to be top brands
were fake in 2016

- Proofpoint⁸

400

businesses
per day targeted by
phishing attacks

- Symantec⁹

270

million
illegitimate Facebook
accounts in 2017

- The Telegraph¹⁰

66%

of spear phishing attacks
on social media opened by
users

Blackhat¹¹

⁸ Proofpoint, 2017, Social Media Protection, Brand Fraud Report

⁹ Symantec, 2018, Internet Security Threat Report

¹⁰ The Telegraph, 2017, 'Facebook admits up to 270m users are fake and duplicate accounts'

¹¹ BlackHat, 'Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter'

Corrata's Mobile Security Solution

Corrata provides protection from phishing attacks by detecting and blocking any attempt to access a malicious site or app. Corrata's Threat Defense solution protects against the full range of phishing attacks on mobile – email, SMS, messaging services, apps and social media. Corrata's protection is based on the latest threat intelligence to ensure even the most recent phishing attacks are protected against.

How it works:

Detect

Detect phishing attempts from any source, including email, SMS and social media

Block

Block access to any suspicious or malicious websites or content

Notify

Notifications sent to the end user to inform them why access was blocked, and the administrators, via the Corrata Console, to inform them of the attempted attack

Corrata's Mobile Threat Defense solution provides mobile devices with all the protection and security afforded to desktops and devices inside the corporate network. Unlike existing anti-phishing filters, Corrata protects from phishing attacks on every platform including social media and messaging apps. The **'Zero Gateway'** architecture of the solution solves the security gap of existing proxy solutions by scanning all mobile traffic in real-time on the device. The employee is always protected regardless of whether they are inside or outside the office and regardless of which platform is used. Corrata's 'Zero Gateway' architecture also addresses the user experience and privacy drawbacks of proxy solutions by processing all data on the device and negating the need for a gateway.

