Lookout®

WHITEPAPER

Mobile phishing 2018: Myths and facts facing every modern enterprise today

Mobile devices have opened a profitable new window of opportunity for criminals executing phishing attacks. Attackers are successfully circumventing existing phishing protection to target the mobile device. These attacks are highlighting security shortcomings and exposing sensitive data and personal information at an alarming rate.

Most corporations are protected from email-based phishing attacks through traditional firewalls, secure email gateways, and endpoint protection. In addition, people today are getting better at identifying phishing attacks. Mobile, however, has made identifying and blocking phishing attacks considerably more difficult for both individuals and existing security technologies.

Phishing is both different and more problematic on the mobile device.

Mobile devices are connected outside traditional firewalls, typically lack endpoint security solutions, and access a plethora of new messaging platforms not used on desktops. Additionally, the mobile user interface does not have the depth of detail needed to identify phishing attacks, such as hovering over hyperlinks to show the destination. As a result, mobile users are three times more likely to fall for phishing scams, according to IBM.

Finally, the huge amount of personal and corporate data on mobile devices, is making these devices the preferred target for phishing attacks.

In fact, in spite of being protected by traditional phishing protection and education, 56% of Lookout users received and tapped a phishing URL on their mobile device between 2011–2016. Fortunately, in these cases the attack was thwarted by Lookout. Unfortunately though, the rate at which Lookout users are receiving and tapping on phishing URLs on their mobile devices has grown by an average of 85% YoY since 2011.

The problem with phishing on mobile is a much more nuanced beast than enterprises realize. Before enterprises can achieve comprehensive protection against phishing attacks across all vectors, including the mobile device, security and IT professionals need to understand how current phishing myths muddy the waters and get the facts that will help them make informed decisions on how to protect corporate data.

The rate at which people are falling for phishing attacks on mobile has increased

85% EVERY YEAR SINCE 2011

56%

of Lookout users received and tapped on a phishing url on mobile

TABLE OF CONTENTS

Phishing on mobile myth #1

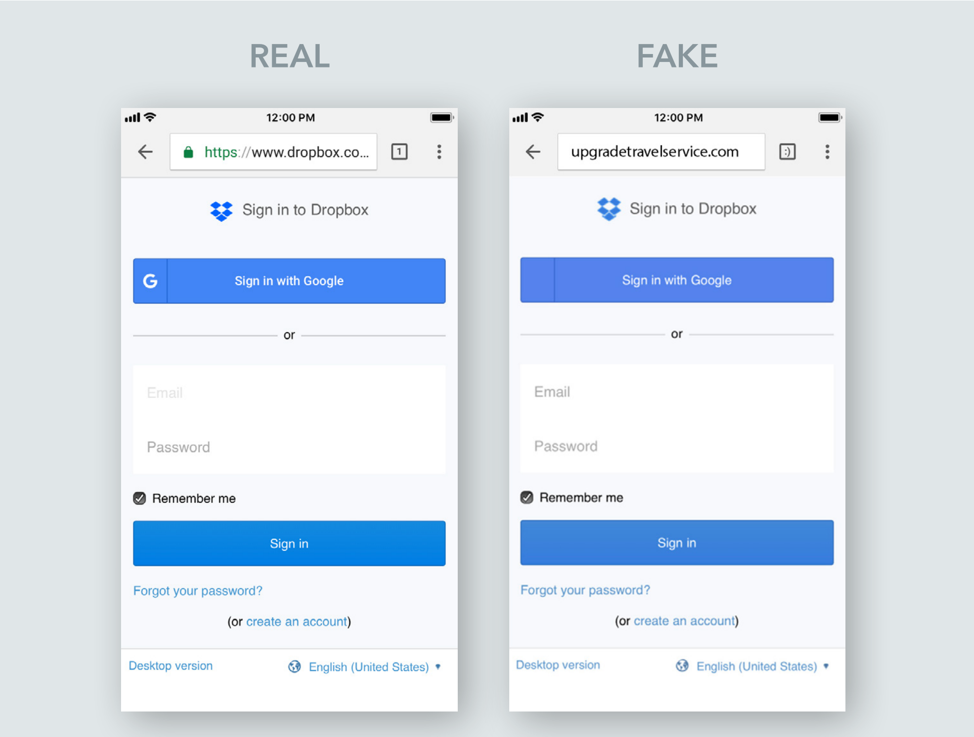
Existing phishing protection is adequate for mobile devices.

Traditionally, corporations have used firewalls, secure email gateways, endpoint antivirus, and user education to prevent employees from receiving or being tricked by phishing messages. This approach works on fixed devices like laptops that are fully corporate-owned and managed. However, as most CISOs know firsthand, mobile devices don't fit into these parameters.

Today, mobile devices, even corporate devices, are also personal devices. An employee often uses the same smartphone for work that is used to pay for lunch, send personal emails, take family photos, check social media, review customer records, get directions to meetings, and skim financial reports. Gaming apps, dating apps, and messaging apps sit next to document readers, corporate email, file-sharing apps, and other apps that contain your company's most important data.

For example, email is arguably the first point of attack for a phishing actor and today over 66% of emails are opened first on a mobile device, according to the U.S. Consumer Device Preference Report from MovableInk. While enterprises have focused on protecting corporate email, personal email on mobile opens a new avenue for attack.

Most reputable personal email providers do have commodity-level phishing protections, but attackers are finding ways to evade these technologies and trick employees into giving over sensitive information or downloading malicious apps. This opens a pathway to corporate data. Savvy attackers are targeting personal email accounts to execute corporate phishing attacks because they know the same stringent protections that are available on corporate email are not on personal email. They also know that both of these accounts are present on the mobile device.



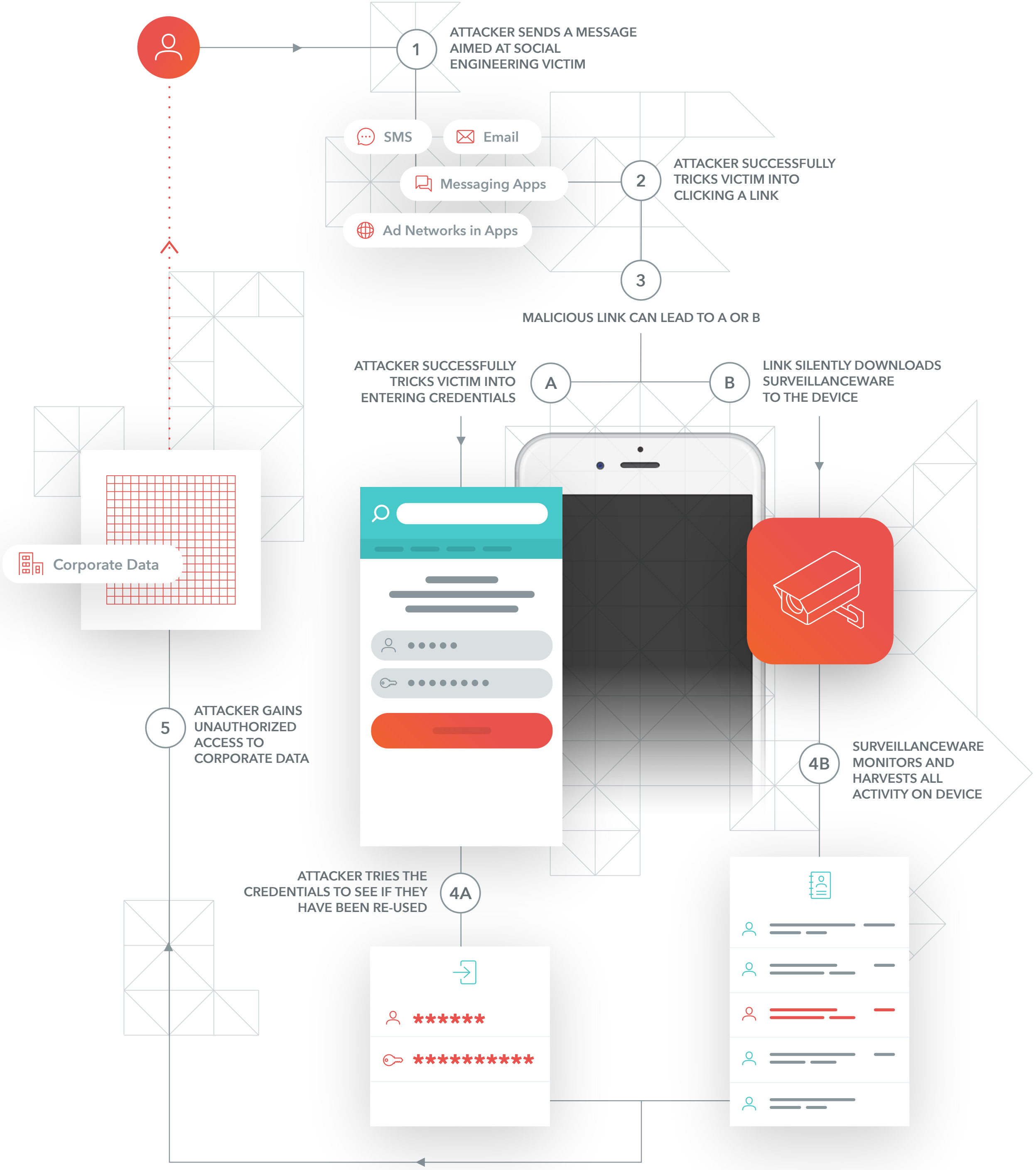
When the address bar disappears to hide the URL, these two log-in pages are virtually identical on mobile.

When you see how convincing phishing sites (or webpages crafted to trick individuals into giving over their information) can be, it's not hard to understand why it's such an effective medium for attackers. A quick look at the following log-in pages highlights the point: determining real from fake can be a difficult task even for experts, and especially on the relatively small screen of a mobile device.

Yet email is only one of the vectors phishing impacts, and mobile devices open up an entirely new realm of access points to attack.

The Mobile phishing kill chain

It only takes one errant tap to compromise a mobile device. That tap may be on a malicious URL that was truncated in the browser window, a URL an app accessed in its backend to unknowingly connect to a malicious ad network, or a link in personal email created to trick a user into offering corporate access credentials – that enables an attacker to move laterally in your infrastructure towards your valuable data.


1
ATTACKER SENDS A MESSAGE AIMED AT SOCIAL ENGINEERING VICTIM
SMS
Email
Messaging Apps
Ad Networks in Apps
2
ATTACKER SUCCESSFULLY TRICKS VICTIM INTO CLICKING A LINK
3
MALICIOUS LINK CAN LEAD TO A OR B
A
ATTACKER SUCCESSFULLY TRICKS VICTIM INTO ENTERING CREDENTIALS
B
LINK SILENTLY DOWNLOADS SURVEILLANCEWARE TO THE DEVICE
Corporate Data
5
ATTACKER GAINS UNAUTHORIZED ACCESS TO CORPORATE DATA
4B
SURVEILLANCEWARE MONITORS AND HARVESTS ALL ACTIVITY ON DEVICE
4A
ATTACKER TRIES THE CREDENTIALS TO SEE IF THEY HAVE BEEN RE-USED
******
****

Phishing on mobile myth #2

Phishing attacks only occur on email.

Contrary to popular belief, phishing attacks are not isolated to email. Mobile devices open entirely new avenues of attack for malicious actors. Attackers now take advantage of SMS and MMS as a means of phishing, as well as some of today's most popular and highly used personal social media apps and messaging platforms such as WhatsApp, Facebook Messenger, and Instagram.

Employees actually fall for SMS phishing attacks. Over 25% of employees clicked on a link in an SMS message from a phone number spoofed to look like one in their area, according to Lookout research.

Security professionals who overlook these new routes of attack put their organizations at risk. A quick look at recent real-world, non-email phishing examples explains why.

ViperRAT

ViperRAT is a sophisticated form of surveillanceware. The threat actors behind ViperRAT lure victims into downloading a malicious app by posing as women on social media platforms. After building a relationship, the attacker sends the victim a message over the social media platform asking them to download an app for "easier communication."

The type of information ViperRAT steals could let an attacker know where a person is, with whom they are associated (including contacts' profile photos), the messages they send, their browser history, screenshots that capture data from other apps on the device, audio spoken or played in the presence of the device, and a myriad of images including anything at which device's camera is pointed.

Learn more about ViperRAT

Facebook Phishing Campaign

Researchers at F-Secure identified a phishing campaign that targeted iOS and Android users. The attacker sent victims a message through Facebook Messenger suggesting that they appeared in a YouTube video. If the victim clicked on the link through an iOS or Android device, it would detect the device-type and specifically serve them a page that looked like the Facebook login page designed to capture the victim's credentials. PC users would receive a different experience. This sort of attack could be used to socially engineer victims into giving over credentials for any service, including those used by enterprises.

Learn more about the Facebook Phishing Campaign

These types of phishing attacks – just a few examples of the many that exist today – prove that attackers are moving beyond email and targeting mobile devices. They also highlight why mobile devices have quickly become a primary vector for such attacks:

- Mobile devices offer new messaging platforms like the ones mentioned above.
- The device is often unmanaged and does not have endpoint security on it, and is therefore less protected from an attack.
- Surveillance is often more effective on mobile because of the capabilities mobile devices offer (e.g., location services, front- and back-facing cameras, microphones, voice calls, text messaging, email, apps) and the fact that people always have their phones on them.

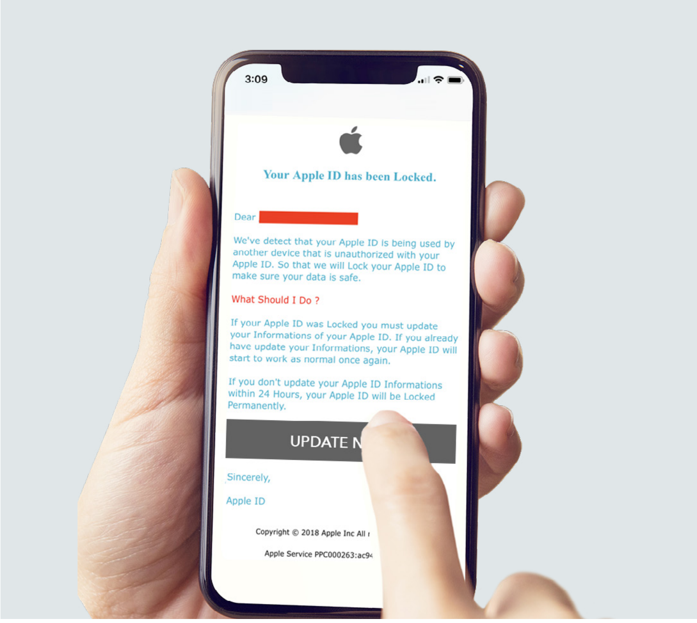
Mobile phishing fact #1

It is easier to trick individuals into falling for phishing attacks on mobile than it is on desktop.

The features, functionality, and even the screen size of today's mobile devices offers attackers an advantage in phishing. Mobile devices make it harder for a person to determine what is real and fake, and operate outside of the traditional corporate security perimeter.

Example 1

Studies have shown that people are three times more likely to click on a suspicious link on a phone than on a PC. Compared to desktop computers where users can "hover" over the hyperlinks to see the complete link, links on mobile are significantly more difficult to verify before clicking on them. Add to that the fact that web views within mobile apps (such as Facebook) also make it near impossible to know which URLs users are visiting, and it becomes clear to see why attackers favor mobile.



3:09

Your Apple ID has been Locked.

Dear [redacted]

We've detect that your Apple ID is being used by another device that is unauthorized with your Apple ID. So that we will Lock your Apple ID to make sure your data is safe.

What Should I Do ?

If your Apple ID was Locked you must update your Informations of your Apple ID. If you already have update your Informations, your Apple ID will start to work as normal once again.

If you don't update your Apple ID Informations within 24 Hours, your Apple ID will be Locked Permanently.

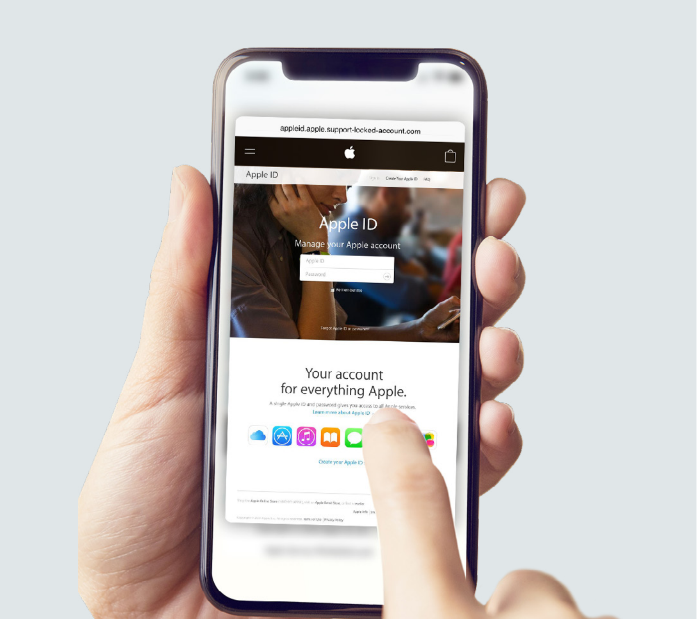
UPDATE N

Sincerely,

Apple ID

Copyright © 2018 Apple Inc All r

Apple Service PPC000263:ac94



appleid.apple.support-locked-account.com

Apple ID

Apple ID

Manage your Apple account

Apple ID

Password

Remember me

Forgot Apple ID or password?

Your account
for everything Apple.

A single Apple ID and password gives you access to all Apple services.

Learn more about Apple ID

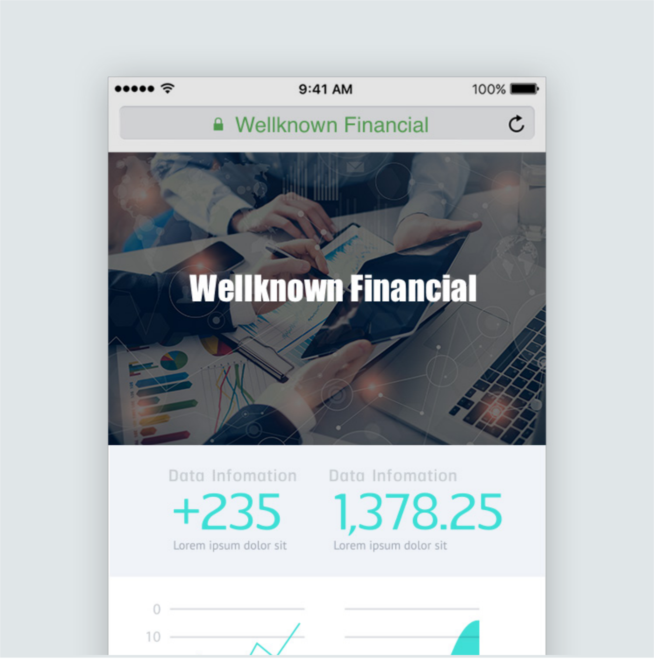
Create your Apple ID

What's going on here: It is very difficult to see where a link leads on mobile. For example, pressing, without tapping, a link on iOS activates 3D-touch, loads the linked page. If an attacker was using a convincingly designed phishing page, the user would still have trouble determining spoofed websites from real ones.

Example 2

When looking at a large monitor screen you may notice that a URL reads "wellknownfinancial.com---------------fakesite.xyz" instead of "wellknownfinancial.com" but because the mobile browser truncates the URL in the address bar, you'll only see "wellknownfinancial.com---" in either case. In some cases the browser will actually replace the URL with the name of the company whose website you are accessing, as seen in the example to the right. This makes it much more difficult to know if the URL is legitimate.

Mobile browsers also often obscure website URLs both by hiding the address bar while a user is scrolling and by limiting the number of characters displayed in the address bar by the width of the screen. In this case, these thoughtful design optimizations enhance an attacker's ability to execute phishing attacks in the open.



What's going on here: The address bar only shows the company name, not the actual URL

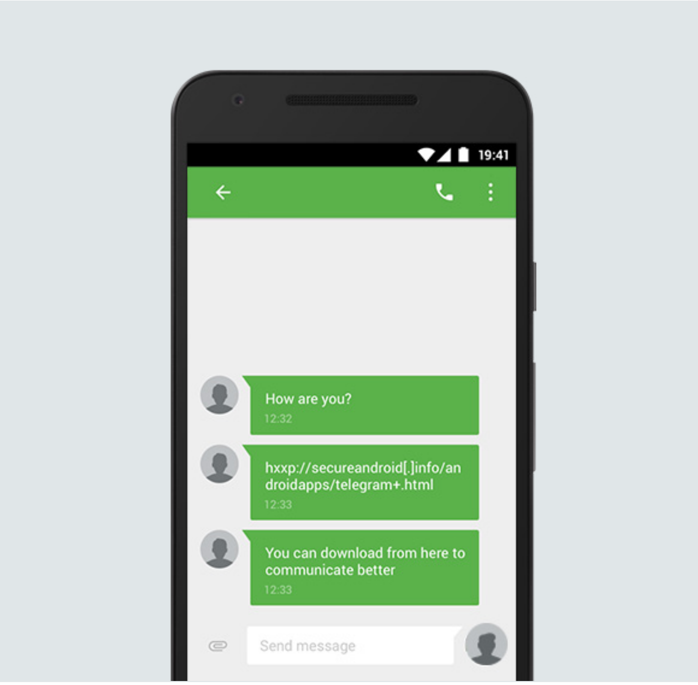
Example 3

When a mobile device is behind a firewall, and a user clicks on a phishing link, the firewall will act to stop the employee from connecting. However, mobile devices are just that – mobile – and, as a result, employees typically spend more time outside the firewall. The mobile device is almost always outside the traditional perimeter, so if an employee encounters a malicious URL (for example, on their commute home) the firewall is no longer there to protect the employee. This makes it easier for attackers to gain unauthorized access if the enterprise only embraces tradition perimeter security.

Mobile phishing fact #2

Mobile malware authors are successfully executing phishing techniques in the wild, especially mAPT actors.

Mobile phishing is increasingly the tip of the spear for sophisticated, large-scale attacks. Some of the most active attacks come from mobile advanced persistent threats, or mAPTs. The term 'Advanced Persistent Threat' is the common way to describe a group, usually a nation-state, that has the capability and intent to persistently and effectively target other nation-states, large enterprises, businesses, or individuals in order to extract information that is typically used for the purpose of financial gain or espionage. An mAPT brings this attack to mobile. Here are a couple of recent examples:

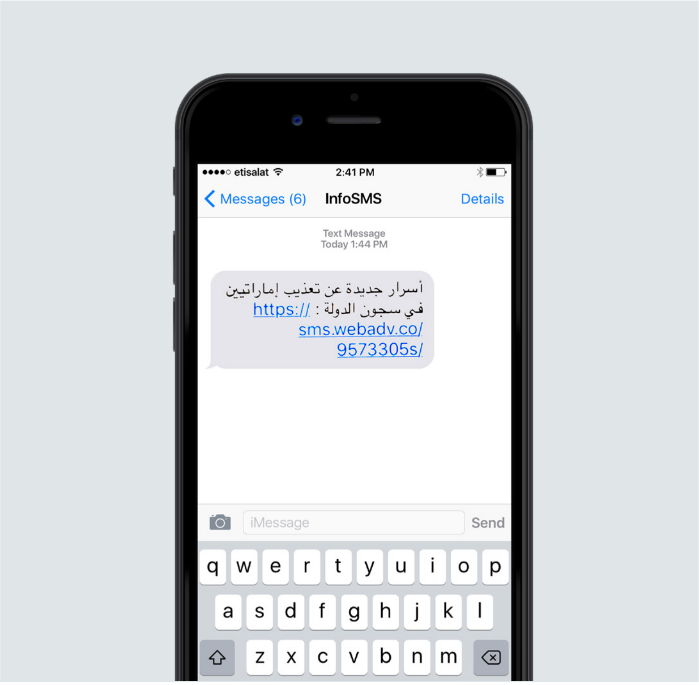


How are you?
12:32

hxxp://secureandroid[.]info/androidapps/telegram+.html
12:33

You can download from here to communicate better
12:33

Dark Caracal SMS message



Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

Pegasus phishing SMS messages captured by Citizen Lab.

- **Dark Caracal**

  Dark Caracal uses phishing messages through WhatsApp and Facebook to lure victims into clicking malicious links and downloading Android malware. The Android malware, called Pallas, then surveils the victim's device, collecting huge amounts of data.

  Dark Caracal targets include governments, militaries, utilities, financial institutions, manufacturing companies, and defense contractors. The types of exfiltrated data is extensive, including documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data.

- **Pegasus**

  The Pegasus surveillanceware received worldwide attention because of its severity. The operators distributing Pegasus sent victims a phishing message via SMS. If the victim clicked, it set off a chain of silent events, leading to one of the most sophisticated iOS device compromise attacks Lookout has seen. Similarly, once on the device, Pegasus monitored all the activity on the device and collected significant amounts of sensitive data.

Awareness is critical because mAPT attacks demonstrate a next-level of sophistication.

Mobile phishing fact #3

Enterprises need to worry about apps (not just people) unknowingly accessing malicious URLs and serving them up to unsuspecting mobile users.

URLs are not only used or accessed (e.g., clicked on) by end users. Apps use URLs in their codebase to communicate and pull down information in real-time. Attackers can use this functionality to phish individuals. This creates a new attack surface for enterprises to worry about: "benign apps" accessing malicious URLs.

For example, apps often use advertising to make money. In order to do so, they incorporate ad SDKs into their code. These SDKs connect to URLs behind the scenes in order to display ads to the end user. If a benign app uses an ad SDK run by an attacker, that attacker may use the SDK to access malicious URLs in order to display ads meant to trick the end user into giving over sensitive data.

While such threats take advantage of "behind the scenes" functionality, not all phishing attacks need to be hidden to be effective.

How Lookout solves the phishing problem

Lookout phishing & content protection, available in Lookout Mobile Endpoint Security, is designed to protect enterprises from phishing attacks in the mobile-first world.

Lookout phishing & content protection

Detect – Detect phishing attempts from any source on mobile devices, including email (corporate or personal), SMS, chat apps, social media, and more, and set policies to protect against phishing attempts.

Protect – Block connections on mobile devices to known malicious URLs hosted on risky websites that may attempt to phish for credentials or attempt to perform other malicious acts.

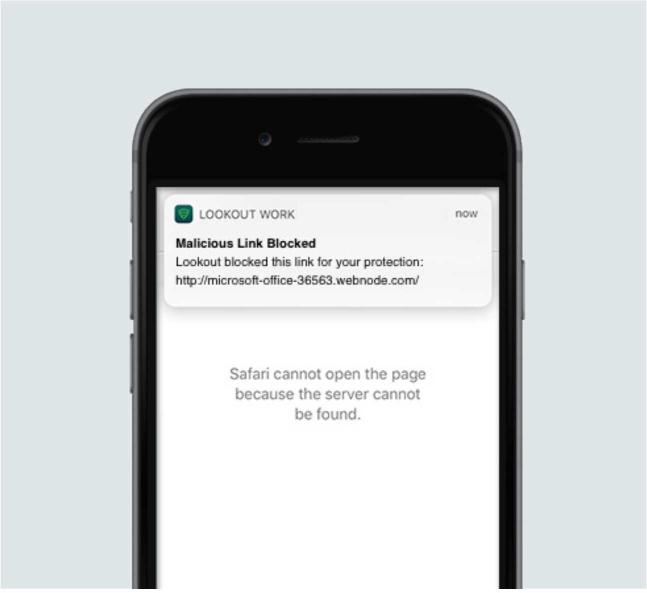
- Malicious URLs include ad fraud, botnets, command and control centers, compromised and links to malware, malware call-home, malware distribution points, phishing/fraud, spam URLs, risky content such as malicious apps or websites with known vulnerabilities, and spyware.

Remediate – Alert end-users at the actual time of URL access.
This real-time alert prevents exposure to the phishing or malicious site.

Analyze – Gain visibility into the frequency and severity of users clicking phishing and malicious links, as well as track whether or not devices have enabled phishing & content protection. Devices that do not have the feature enabled are marked as out-of-compliance allowing for typical enterprise remediation through integration to leading EMM vendors.

How it works

Lookout phishing & content protection blocks any attempted connection to malicious and phishing URLs, at the network level, when the device or employee attempts to connect. What's important and different about this approach is that it does not rely on inspecting the message content. Many social and messaging platforms used on mobile devices such as SMS, WhatsApp, Facebook Messenger, and personal email are highly sensitive and private to the user. By only inspecting the URL at the time the individual or device attempts to connect, Lookout phishing and content protection maintains user privacy. By inspecting these URLs at the network level, Lookout is able to protect users from connecting to malicious or phishing URLs from any email, text message, social network, or any other app.



LOOKOUT WORK now

Malicious Link Blocked
Lookout blocked this link for your protection:
http://microsoft-office-36563.webnode.com/

Safari cannot open the page because the server cannot be found.

The benefits of Lookout phishing & content protection

Lookout Mobile Endpoint Security has always worked to make it easy to get visibility into your organization's entire Spectrum of Mobile Risk, apply policies to measurably reduce that risk, and integrate into your existing security and mobile management solutions. Now with our phishing & content protection feature, you will benefit even more. The feature:

Adds a powerful line of defense against phishing attacks and malicious websites, extending phishing protection to mobile across email, social, and messaging platforms.

Provides comprehensive protection on the "web and content" threat vector in the Spectrum of Mobile Risk, one of the most prevalent mobile vectors used by attackers to exfiltrate enterprise data.

Enables organizations to confidently embrace the use of smartphones for work by protecting against malicious content whether the employee is inside the protected corporate network or not.

Maintains end-user privacy by adhering to data minimization and purposeful data collection principles, including robust privacy controls and the ability to restrict collection of PII associated with users or devices.

When you equip yourself with Lookout Mobile Endpoint Security, including phishing & content protection, you give your organization a proven way to mitigate risk and securely enable mobility within your enterprise.

Offering real protection in action

Mobility has transformed the enterprise – literally changing how work gets done. Organizations are actively seeking ways to promote employee productivity and flexibility while keeping sensitive data, employee and customer information, and critical network infrastructure secure.

- Lookout phishing & content protection responds to practical needs and actual problems faced by administrators on a daily basis.
- Administrators want to allow employees to freely browse the web on their mobile devices, but also want to block websites known for malicious activity.
- Administrators are concerned that employees use various browsers on mobile devices and are not warned of risky websites, so they want to ensure a warning is issued on mobile before users are allowed to proceed.
- Security departments want protection parity across all their endpoints and this fills their mobile gap.
- IT departments will not have to backhaul traffic, effectively putting mobile devices behind a firewall, which offers poor experience and performance issues for employees. Our solution, instead, enables enterprises to fully embrace digital transformation, giving employees a safe way to work with their mobile devices whether they are BYOD or COPE.

Lookout Mobile Endpoint Security was developed to guard against the genuine security challenges mobility introduces to the enterprise. This latest feature allows IT and security professionals to respond to the problems phishing on mobile presents.

Take the next step: Learn how Lookout can help

Malicious actors are using sophisticated forms of phishing to gain entry behind the closed doors of the enterprise.

While security and IT professionals generally recognize the dangers associated with phishing attacks, a majority of organizations have chosen to focus securing traditional endpoints, like PCs. This is not enough.

Phishing is both different and more problematic on the mobile device than traditional endpoints. Enterprises seeking comprehensive protection against phishing attacks across all vectors, including the mobile device, need to look beyond status quo options. Lookout Mobile Endpoint Security offers the next level of defense required.

To learn how you can secure your mobile fleet today, contact us at info@lookout.com

*About the data: The data above is from an analysis of 67M mobile devices protected by Lookout Personal between 2011 and 2016. All data is anonymous, and no corporate data, networks, or systems were accessed to perform this analysis.