wandera

MAY 2018

Mobile phishing report 2018

Mobile phishing is now the number one threat affecting organizations worldwide. This whitepaper will look at the evolution of mobile phishing - examining why and how people get phished. It will explore the prevalence and severity of enterprise phishing techniques, providing actionable advice for how best to protect your mobile device fleet.

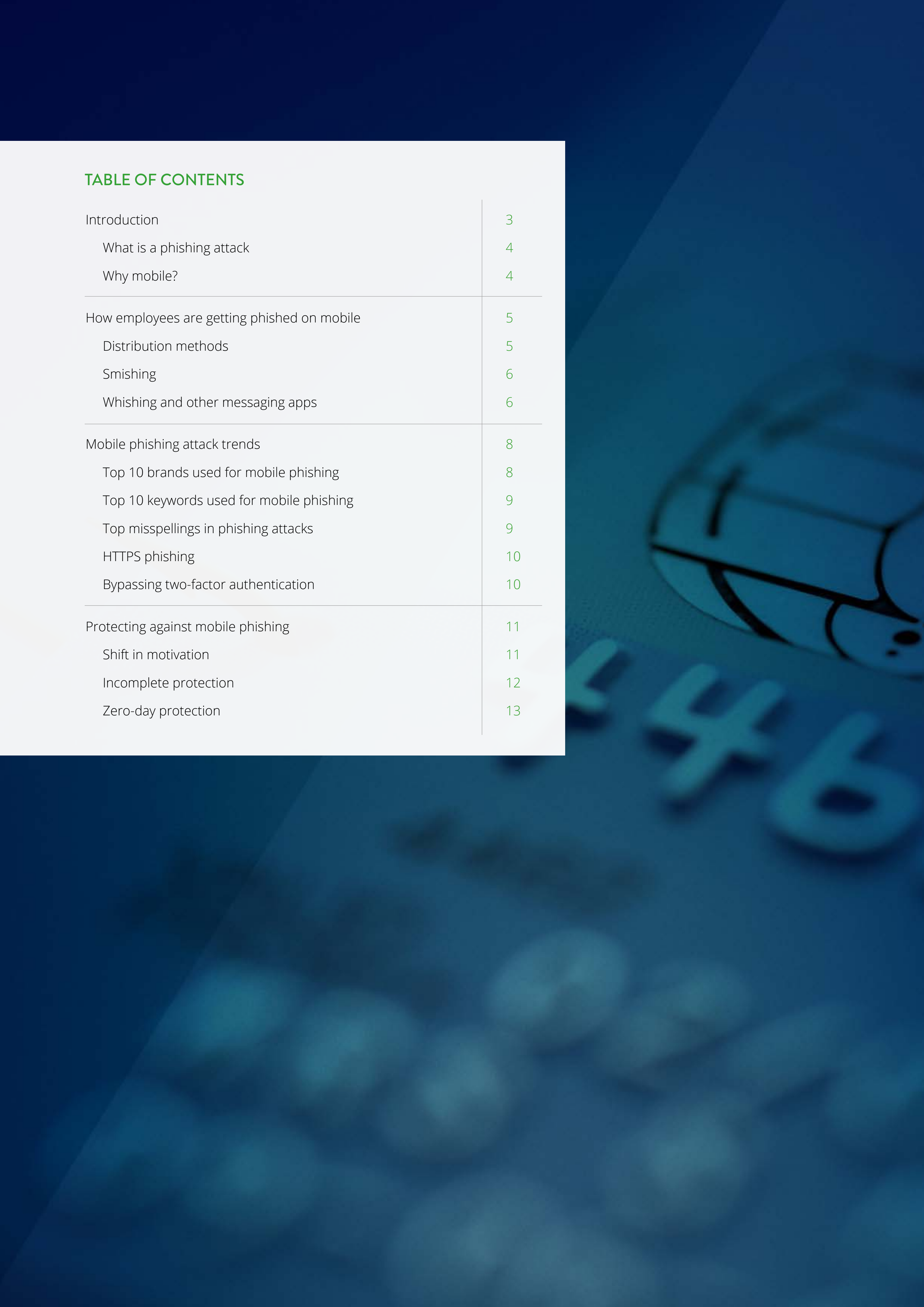


TABLE OF CONTENTS

Introduction

Several decades ago when the public took to the web in their masses to experience the benefits of interconnectedness, cyber attacks were practically unheard of. However, things soon changed. Early adopters of the web quickly realized that the online world could give them something that was more difficult to find offline: anonymity. While in many aspects this was viewed as a positive thing, a handful of users took a more cynical approach.

Individuals learned that through employing some relatively simple techniques, it was possible to impersonate third parties, gather intelligence and earn a sizeable sum in the process. Internet phishing was born.

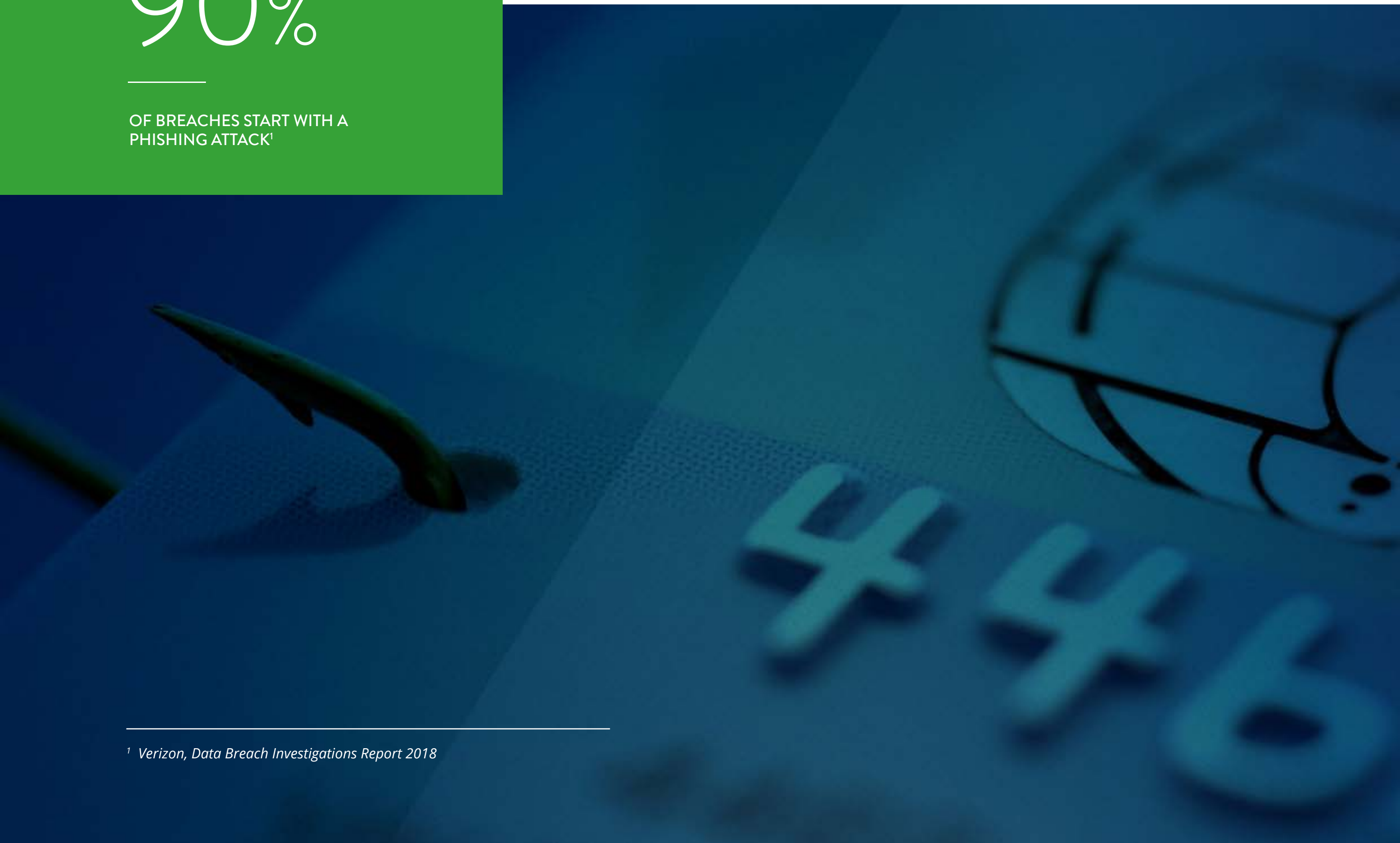
Fast forward to 2018 and phishing attacks have evolved beyond all recognition. Phishing is not only regular, but it's also the most damaging and high profile cybersecurity threat facing enterprises today - supported by research from Google, Black Hat and US Homeland Security.

But just how prevalent is mobile phishing? And what techniques are attackers employing to get their hands on your data? This report aims to answer these questions as it delves deeper into the current mobile threat landscape, examining the sophisticated attack techniques targeting businesses across the globe.

> *Phishing is one of the top attack vectors within the enterprise at the moment. The explosion of mobile devices mean they're increasingly attractive targets for attackers.*
>
> - MATT BROOKS, SENIOR PRODUCT MANAGER AT CITRIX

90%

OF BREACHES START WITH A PHISHING ATTACK[1]



[1] *Verizon, Data Breach Investigations Report 2018*

What is a phishing attack?

Phishing is a simple yet effective attack technique, which can provide the perpetrators with a wealth of personal and corporate information.

The attack itself usually begins with a form of communication to an unsuspecting victim: a text, an email, or message via an in-app inbox. The message is engineered to encourage user interaction with an enticing call to action. Perhaps the chance to win a new iPhone, holiday vouchers or more simply, the opportunity to gain access to a service like Facebook.

The aim and precise mechanics of the attack can vary, but they commonly center around either extracting personal data from the victim or getting them to install malicious software that can inflict damage upon their device.

Why are phishing attacks so dangerous? Well, they exploit the most vulnerable part of an organization: its employees. Employees are often a corporation's most valuable asset, but when it comes to keeping data safe they double up as their biggest security weakness. Even the most vigilant team members respond to cleverly targeted phishing campaigns, click on files riddled with malware and open attachments from "colleagues" without giving it a second thought.

> *"Mobile phishing is relentless within the enterprise and we don't expect this to change any time soon. Unsuspecting victims are encouraged to click links, or run files to launch malicious code to start the attack. "*
>
> - SACHIN SHARMA, PRODUCT MARKETING AT VMWARE

Why mobile?

Mobile is the new frontier for cybercrime. In fact, a huge 48% of phishing attacks are on mobile according to Cloudmark and the number of mobile phishing attacks is doubling every year. Mobile phishing is so rife that a new type of attack is launched once every 20 seconds. That's more than 4,000 new mobile phishing attacks per day and that's not taking into account the millions of existing phishing pages. Phishing sites morph, evolve and redirect by the second, and over time can be reused again and again to target different organizations and individuals.

Why are these numbers so high? Well it's easier for an attacker to exploit a person via a phishing attack, than it is to exploit the relatively robust mobile operating systems - especially iOS.

Most web traffic now happens on mobile. Therefore it doesn't come as a shock that hackers use this to their advantage by crafting attacks specific to a mobile platform. Mobile devices have smaller screens and feature a number of visual shortcuts, meaning spotting suspicious URLs or malicious senders is far more difficult than on desktop. Users are also more distracted and vulnerable on mobile devices due to their portable nature and inherently personal feel.

18x

A mobile user is 18x more likely to be exposed to a phishing attempt than malware. *Less scrutinized channels like SMS, Skype, WhatsApp, games and social media are being leveraged at scale to distribute phishing links in places employees do not expect.*

Distribution methods

With more than 4,000 new mobile phishing sites being created every day, mobile phishing is clearly a common and successful form of attack. It's also clear that hackers have moved on from the trusted domain of email, and onto the multitude of new distribution methods made available by the explosive availability of mobile devices in recent years.

Phishing attacks are everywhere, and make use of layered, multi-touch distribution channels. While email remains the No.1 target of phishers, email filters and decades of training mean that these attacks are seldom effective. When looking at actual live successful attacks, fewer than 1 in 5 originate from email phishing campaigns.

Wandera research focused on analysis of the traffic to known phishing domains and, due to Wandera's unique cloud infrastructure that offers full visibility into device traffic, researchers were able to determine which apps and services are used to distribute the phishing attacks. The following data has been gathered from a sample of 100,000 Wandera-enabled devices for a four week period in March 2018.

Beyond email: the explosion of phishing from messaging and social media applications

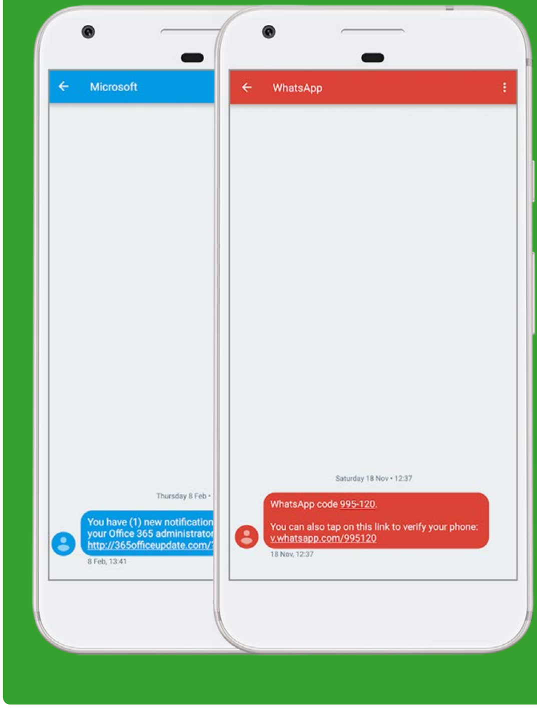
17.3%	Messaging	▲ +170% INCREASE ON 2017
16.4%	Social Media	▲ +102% INCREASE ON 2017
15.4%	Email	
11.3%	Gaming	
10.2%	Productivity	
6.3%	Sports	
6.1%	Dating	
5.3%	Ecommerce	
3.0%	News and weather	
2.2%	Food and drink	
2.1%	Health and fitness	
2.1%	Travel	
1.3%	Music	
1.0%	Finance	

Smishing

Security systems pointed at traditional architecture – desktop, for example – are typically well resourced and robust at defending against attacks. Text messages on mobile tend to be an overlooked area in a CISO's strategy, and thus make for lucrative phishing waters for attackers. It's also remarkably easy to emulate the sender information to make it look like messages are sent from a trusted service.

This impact is amplified by the notion that very few individuals know the phone number of their ISP, banking provider or cloud storage account, meaning inspection of the sender address is unlikely to arouse suspicion. With SMS phishing (also known as 'smishing'), if a message looks like it comes from Microsoft, for most people there's little reason to think otherwise. Victims are then directed towards a fake landing page, designed to harvest user credentials.

SMISHING IN THE WILD - MICROSOFT AND WHATSAPP



Thursday 8 Feb •

You have (1) new notification
your Office 365 administrator
http://365officeupdate.com/

8 Feb, 13:41

Saturday 18 Nov • 12:37

WhatsApp code 995-120.

You can also tap on this link to verify your phone: v.whatsapp.com/995120

18 Nov, 12:37

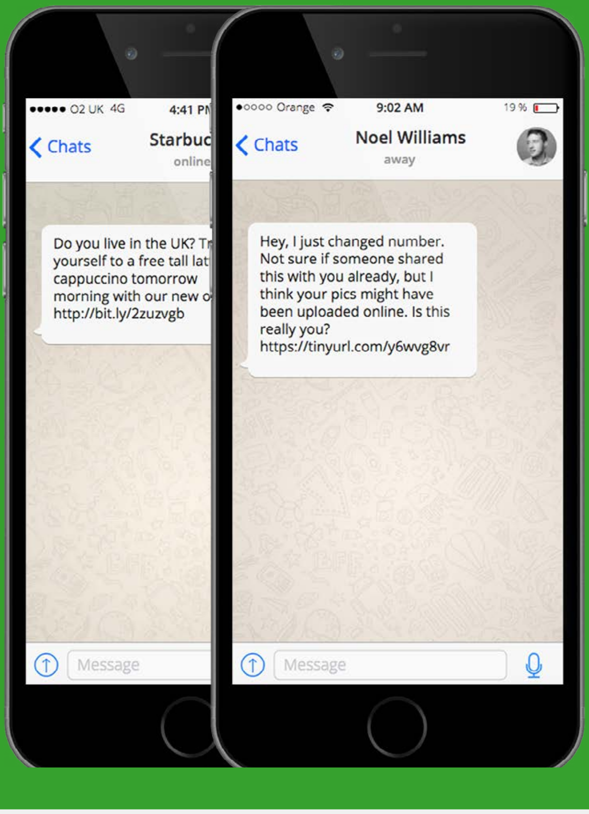
Whishing and other messaging apps

It's not only through SMS that phishers are able to reach their targets with surreptitious links. WhatsApp is another powerful channel for distributing phishing attacks, with hackers able to create profiles disguised to look like legitimate senders.

Once again, as most people are not familiar with the official accounts of various brands, profiles that feature a legitimate-sounding name and logo are much more convincing than an email from an unknown address. The rise of WhatsApp phishing, or 'whishing', has seen a growth in campaigns that offer promotional deals, often pretending to be from well-known brands like McDonalds, Nike or supermarket chains.

In some cases these attacks will be more focused and instead used in targetted spear phishing. These attacks involve the impersonation of a known individual, which with some quick internet research can be easily mimicked to build a misplaced sense of trust in the target – again exploiting the employee in order to extract data.

PHISHING IN THE WILD



Do you live in the UK? Tr
yourself to a free tall lat
cappuccino tomorrow
morning with our new o
http://bit.ly/2zuzvgb

Hey, I just changed number. Not sure if someone shared this with you already, but I think your pics might have been uploaded online. Is this really you? https://tinyurl.com/y6wvg8vr

THE TOP 5 APPS FOR MESSENGER PHISHING

1 Messenger

2 WhatsApp

3 Facebook Messenger

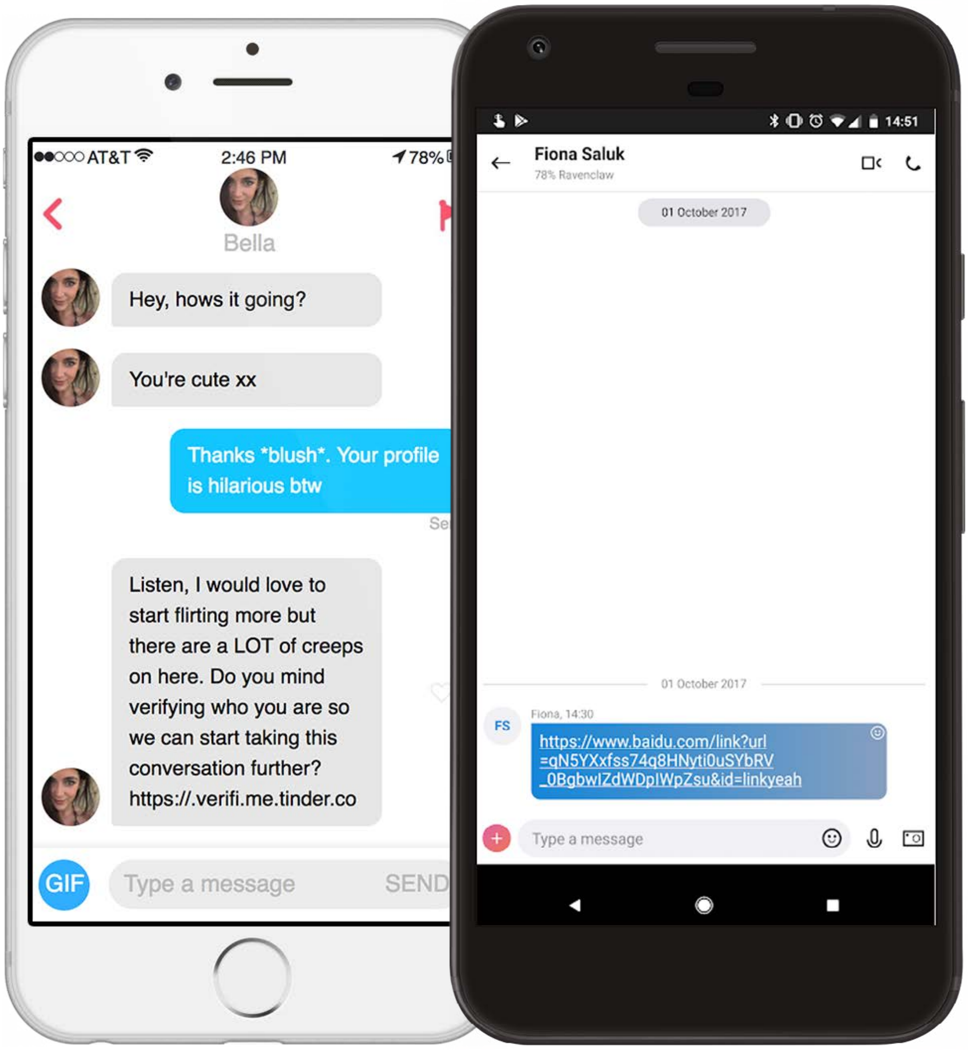
4 LINE

5 Viber

Worryingly, these attacks are everywhere. There is nothing wrong with WhatsApp itself, and so locking down access simply moves the problem, rather than solve it. More importantly, it's not just SMS and WhatsApp that feature in the mobile phisher's toolkit. With literally thousands of messaging apps to choose from, phishing attacks could happen almost anywhere.

Research at Wandera uncovered instances of employees navigating to phishing URLs through dating apps like Tinder and Happn. In fact, analysis of phishing activity on thousands of employee devices suggests that over 6.1% of all successful mobile phishing attacks take place on dating apps.

Phishing attacks have been observed in practically every single form of communication on mobile devices, including Skype, QQ, WeChat, Viber and Kik. Clearly this is a problem at scale that cannot be solved through blocking certain apps, or through app-centric controls.



Hey, hows it going?

You're cute xx

Thanks *blush*. Your profile is hilarious btw

Listen, I would love to start flirting more but there are a LOT of creeps on here. Do you mind verifying who you are so we can start taking this conversation further? https://.verifi.me.tinder.co

https://www.baidu.com/link?url=qN5YXxfss74q8HNyti0uSYbRV_0BgbwIZdWDpIWpZsu&id=linkyeah

Mobile phishing attack trends

The previous examples highlight how attackers are not short of distribution vehicles for their phishing campaigns. Utilizing a range of communication platforms is one thing, but in order to increase the success rate of an attack, malicious actors need to be selective when deciding which companies to impersonate.

It's simple - reputable brands with a large user communities are less likely to arouse suspicion as the victim may already receive regular communication from the service. In order to better understand current attack trends MI:RIAM - Wandera's machine learning and intelligence engine - ran an analysis of the top 10 brands targeted by phishing attacks, through an analysis of their unique fully qualified domain names (FQDNs).

Top 10 brands used for mobile phishing

1	2	3	4	5	6	7	8	9	10
Facebook	Apple	Google	Amazon	PayPal	UK Gov	Microsoft	Fox News	Dropbox	Whatsapp

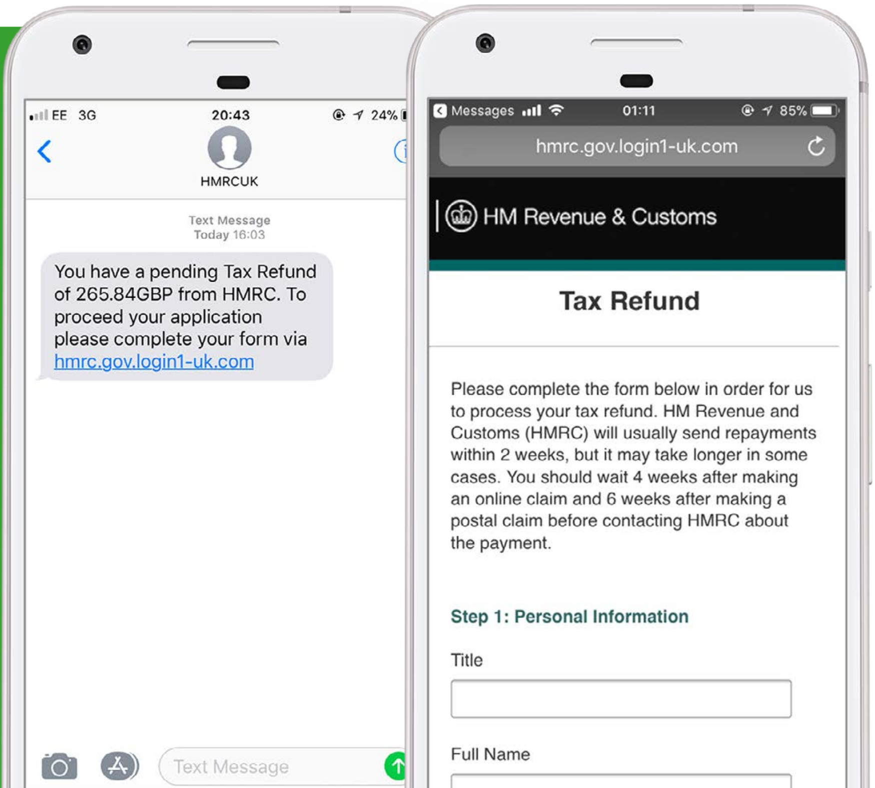
Each of these brands elicit trust on the part of the user. They are online tools and platforms employees interface with regularly on mobile devices. Hackers of course, know and exploit this trust. They create domains that contain these brand names to increase the chances of the user providing the site with their personal information. And the thing is, users are falling for it.

PHISHING IN THE WILD: HMRC AND IRS

Sophisticated attackers may leverage global events to add credence to their phishing campaigns.

MI:RIAM recently detected and intercepted traffic in transit between a device and a malicious third party, after an employee at a global consultancy firm fell for this tax scam.

The SMS was sent shortly after the end of the financial year when government organizations would usually start communicating with the public about tax rebates.



You have a pending Tax Refund of 265.84GBP from HMRC. To proceed your application please complete your form via hmrc.gov.login1-uk.com

Tax Refund

Please complete the form below in order for us to process your tax refund. HM Revenue and Customs (HMRC) will usually send repayments within 2 weeks, but it may take longer in some cases. You should wait 4 weeks after making an online claim and 6 weeks after making a postal claim before contacting HMRC about the payment.

Step 1: Personal Information

Title

Full Name

Top 10 keywords used for mobile phishing

In order to better understand the syntax of a phishing attack the below list outlines the top keywords used within the FQDNs of sites deemed by MI:RIAM as phishing-based on their score.

Of course, this list includes some of the most commonly used terms most of us see in URLs when a site is looking to have us 'login', 'secur*' or 'verif*' our 'account'. We also regularly click on links sent to us from legitimate platforms to 'update' our 'service' or 'authorize' and 'confirm' the login of a user.

RANK	KEYWORDS
1	Account
2	Secur*
3	Verif*
4	Com-
5	Update
6	Support
7	Service
8	Login
9	Auth*
10	Confirm

* *Any word beginning with these letters*

Top misspellings in phishing attacks

Next MI:RIAM analyzed the most common misspellings used in phishing attacks. In this case, hackers are hedging their bets on you casually overlooking the subtle abnormalities in their malicious URLs. It's a technique so popular that it's referred to by several names - URL hijacking, typosquatting even a sting site.

Think about the number of times you've misspelled a domain when you've typed it into your browser, especially when you've entered it on your phone (with a small keyboard and even smaller font size).

Now imagine analyzing each link you click on in your mobile browser window. Remember, these windows cut off at a certain point. So when you look at:

www.amazon.com/home....

www.arnazon.com/home...

There really isn't much of a difference unless you're looking very, very closely. Then you can see the second address uses an 'r' and an 'n' in place of the 'm'.

TARGET/KEYWORD	TOP MISSPELLINGS
1. apple.com	apple-com, applecom, apple.con, appie.com app-le.com
2. paypal.com	pavpal.com, puaypal.com, pauypal.com, paypal-com, paypai.com
3. wells.fargo.com	wellsf.argo.com
4. icloud.com	Iclod.com, icloud-com, 1cloud.com, lcloud.com
5. appleid	apple-id, apple.id, appleld, appieid, applid
6. facebook	facbook, ficebook, faceboook, facebo0k, faceebook
7. amazon	amazo, amazn, a-mazon, amzon
8. microsoft	microsft
9. google	gooogle, gogle
10. americanexpress	americaexpress

HTTPS phishing

Wandera's recent mobile phishing research also highlights another attack trend that is worth looking at in more detail. A number of phishing sites are utilizing HTTPS verification to conceal their deceitful nature. How does this work? Well, SSL certificates are a way of digitally certifying the identity of a website and securing its traffic.

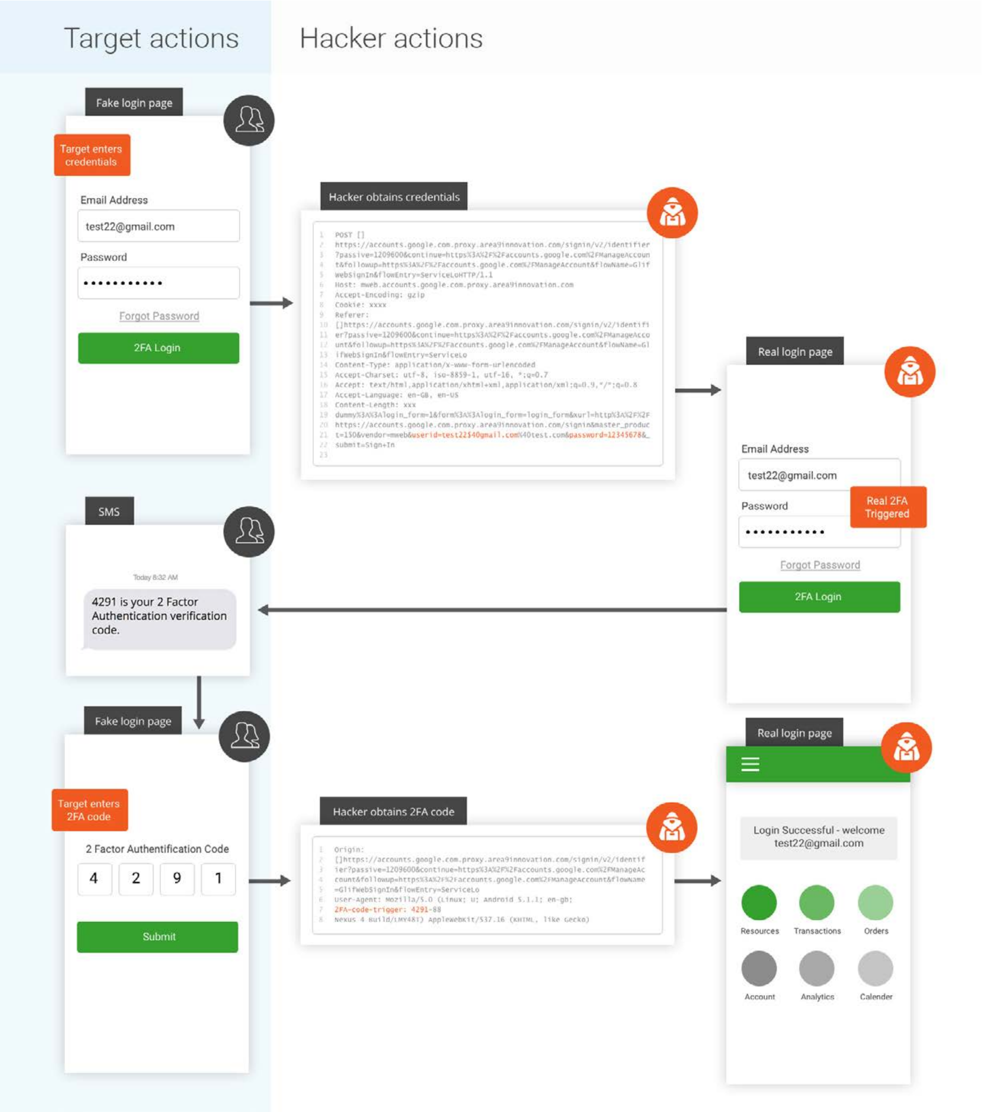
They inform the user that their personal information has been encrypted into an undecipherable format that can only be returned with the proper decryption key. Countless cybersecurity campaigns advocate encryption and tell enterprises that HTTPS sites are the ones to trust, so what's the problem? Exactly that.

Users perceive HTTPS sites to be secure, so they're less likely to suspect a 'phish'. Realising this, hackers use sites like letsencrypt.org to gain SSL certification for their insecure phishing sites. Throughout 2017, the number of phishing sites operating from a secure HTTPS domain skyrocketed, growing by over 1000% and it's a trend we expect to continue as attackers improve their techniques.

ONE SECURE 'HTTPS' PHISHING SITE IS CREATED EVERY TWO MINUTES

Bypassing two-factor authentication

It's become clear that malicious entities are using fake login pages to bypass two-factor authentication. How do they do this? Well in short, the attacker captures your information on a fake page whilst simultaneously entering your credentials into the official site. Worryingly, this process can be automated to carry out an attack on an organization at scale.



test22@gmail.com

••••••••••••

```
POST []
https://accounts.google.com.proxy.area9innovation.com/signin/v2/identifier
?passive=1209600&continue=https%3A%2F%2Faccounts.google.com%2FManageAccoun
t&followup=https%3A%2F%2Faccounts.google.com%2FManageAccount&flowName=Glif
WebSignIn&flowEntry=ServiceLoHTTP/1.1
Host: mweb.accounts.google.com.proxy.area9innovation.com
Accept-Encoding: gzip
Cookie: xxxx
Referer:
[]https://accounts.google.com.proxy.area9innovation.com/signin/v2/identifi
er?passive=1209600&continue=https%3A%2F%2Faccounts.google.com%2FManageAcco
unt&followup=https%3A%2F%2Faccounts.google.com%2FManageAccount&flowName=Gl
ifWebSignIn&flowEntry=ServiceLo
Content-Type: application/x-www-form-urlencoded
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB, en-US
Content-Length: xxx
dummy%3A%3Alogin_form=1&form%3A%3Alogin_form=login_form&xurl=http%3A%2F%2F
https://accounts.google.com.proxy.area9innovation.com/signin&master_produc
t=150&vendor=mweb&userid=test22$40gmail.com%40test.com&password=12345678&_
submit=Sign+In
```

test22@gmail.com

••••••••••••

4291 is your 2 Factor Authentication verification code.

4 2 9 1

```
Origin:
[]https://accounts.google.com.proxy.area9innovation.com/signin/v2/identif
ier?passive=1209600&continue=https%3A%2F%2Faccounts.google.com%2FManageAc
count&followup=https%3A%2F%2Faccounts.google.com%2FManageAccount&flowName
=GlifWebSignIn&flowEntry=ServiceLo
User-Agent: Mozilla/5.0 (Linux; U; Android 5.1.1; en-gb;
2FA-code-trigger: 4291-88
Nexus 4 Build/LMY48T) AppleWebKit/537.16 (KHTML, like Gecko)
```

Login Successful - welcome test22@gmail.com

Protecting against mobile phishing

Shift in motivation

Historically, attackers set out to retrieve information which they could instantly use against the victim - like account credentials and basic personal data. This meant that in most cases, an attacker would infiltrate an organization shortly after harvesting sensitive employee data. However, the mobile phishing landscape is rapidly changing and attackers are taking their time to intricately research their victims for maximum impact. They're profiling victims by gaining the personal data prior to orchestrating an attack.

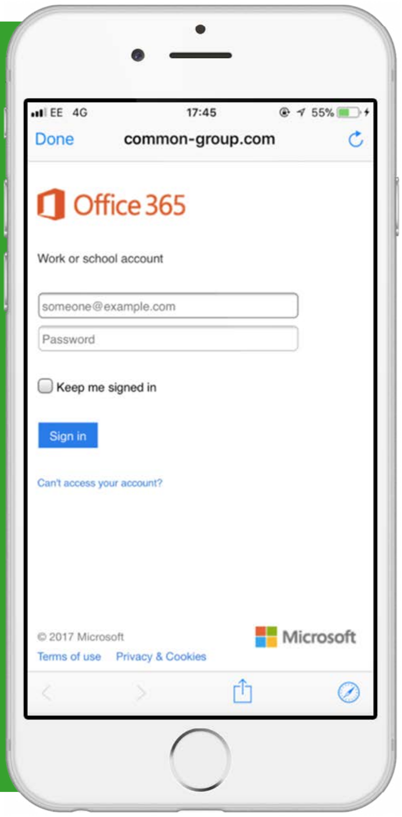
As a result, selling organizational data on the Dark Web has become a lucrative pursuit. Underground markets sell full identities of individuals, and organizations for as little as $10 a piece, but this can quickly add up. This information is referred to by the community as 'fullz' - details that provide enough financial, geographic and biographical information on a victim to facilitate identity theft or other impersonation-based fraud.

In some instances the attacker doesn't have to look very far for your PII. Data is power and once an attacker has your email address, it only takes a quick search on Twitter or Facebook to retrieve more information that they can use against you.

PHISHING IN THE WILD: MICROSOFT OUTLOOK

MI:RIAM recently detected and stopped a phishing attack that attempted to harvest the data of a CMO from a financial services firm that is a customer of Wandera. The attacker used information publicly available on the employee's Twitter page to power their communication.

Noting that the CMO had recently been to a conference, they sent a WhatsApp message that appeared to come from a colleague asking if the recipient would like to see the official event photos. They were then taken to what looked like a Microsoft Outlook login page, but was actually just an imitation. As the company had Wandera in place the traffic was intercepted in transit, but without this level of visibility the attacker would have had complete access to details submitted.



If attackers get their hands on personal employee data from a corporate device, your organization will be held responsible. Not to mention the impact if they are successful in their attempt. Google and Facebook were phished for over $100m back in 2017, proving not even the biggest technology companies in the world are immune to the increasingly sophisticated attacks of online scammers.

Incomplete protection

When it comes to protecting your device fleet against the ever-growing threat of phishing there are a number of things organizations can do. Part of the issue is infrastructure, part of the problem is education.

Employee training

THE SOLUTION	THE PROBLEM
Organizations are investing in user education to discourage employees from clicking on malicious phishing links that expose their information to malicious third parties.	Organizations have learned through experience that education is not enough. The human element leaves room for error and therefore, potential damage to the user and business.

Anti-phishing services

THE SOLUTION	THE PROBLEM
Some companies use anti-spam solutions to block junk mail and phishing attacks from reaching employee inboxes.	Anti-spam solutions that block phishing attempts in e-mail are not adequate. These tools do not address phishing attacks that are distributed outside of email (e.g., in SMS or through social media apps).

App-based security solutions

THE SOLUTION	THE PROBLEM
App-only solutions can detect threats when the device is compromised or when malicious apps are installed. These solutions could allow users to submit questionable SMS messages.	More than 90% of phishing attacks are missed because they do not actually compromise the device or involve malicious apps. The vast majority of phishing attempts take place in the web browser or via apps, such as WhatsApp or Facebook. App-only solutions have limited visibility into phishing attacks that take place through these channels.

Zero-day protection

Many phishing sites are published online for only a few hours before hackers move to an entirely new hosting server. This allows them to evade detection and maintain an ongoing campaign without being detected and blocked. The risk to users is highest in those first critical hours before third-party threat intelligence is updated. In this short window of time, mobile devices are most vulnerable to newly published attacks.

This is why at Wandera we've advanced MI:RIAM's phishing detection algorithms with next-generation machine learning that proactively seeks out new phishing attacks that can be blocked before they hit their first 'patient zero'. MI:RIAM's zero-day phishing algorithm is complex, and relies on a variety of input factors to determine if web content poses a risk to mobile users. Numerous points of data are analyzed and taken together to generate a risk score which ultimately determines if the page is to be flagged and blocked.

Not only that, but this component of MI:RIAM's intelligence is continuously improving. As the algorithm successfully identifies more unique phishing attacks, sitting directly in the pathway of mobile data, it is able to learn more about the anatomy of the attack. This allows it to hone its technique as time goes on and improve its accuracy.

Zero-day phishing intelligence powered by MI:RIAM

Wandera is the only dedicated web gateway for mobile, operating directly in the pathway of mobile data. The solution's unique architecture allows it to sit between the device and the internet, giving it the ability to intercept traffic to phishing sites, whether initiated over SMS, instant messenger or social media applications.

Our mobile intelligence engine MI:RIAM analyzes billions of mobile inputs each day using a wide range of data science techniques. When it comes to phishing, MI:RIAM has a proven industry-leading 98% efficacy of recognizing and proactively blocking mobile phishing attempts.

> *"Our mobile intelligence engine MI:RIAM analyzes billions of mobile inputs each day using a wide range of data science techniques. When it comes to phishing, MI:RIAM has a proven industry-leading 98% efficacy of recognizing and proactively blocking mobile phishing attempts."*
>
> - MICHAEL COVINGTON - VP OF PRODUCT STRATEGY AT WANDERA.

There is no other solution available that can detect mobile traffic directed towards phishing sites, let alone block it. To find out how you can protect your organization from the rising threat of mobile phishing, get in touch with us today.

wandera.com/demo

wandera

Wandera is the global market leader in enterprise mobile security, delivered through its pioneering web gateway. Providing maximum visibility into mobile data, Wandera goes beyond threat detection to prevent attacks and contain data leakage. The solution's threat intelligence is powered by MI:RIAM, a real-time security engine that analyzes the industry's largest mobile dataset to uncover new vulnerabilities and zero-day threats as they emerge.