

The mobile threat landscape

● JAMF
NATION
LIVE

Agenda

1 | Why is mobile at risk?

Why are mobile devices being targeted, and who's targeting them?

2 | Mobile threats in detail

What sorts of mobile threats are there, and what risks do they pose?

3 | How to stay protected

Introducing Jamf Threat Defense, MI:RIAM and the Jamf Trust app



Why is mobile at risk?

Why are mobile devices being targeted, and who's targeting them?

Mobile threats are the modern reality

2.5 million

mobile users downloaded multiple malware apps last year.

6.5%

of all mobile devices are running an out-of-date or vulnerable OS.

85%

of mobile apps are unsecured and leak data.

25%

of all data breaches involve phishing.



Why is mobile being **targeted**?



The footprint of **mobile in business** continues to grow

71%

of organisations rate mobile 8/10 or above in terms of being crucial to their business.

Mobile is becoming increasingly critical in business

24%

sacrificed the security of mobile devices to facilitate their response to the pandemic and its restrictions.

Expansion of the attack surface

In 2021

1 in 10

users fell victim to a **mobile phishing attack**.

39%

of organisations were regularly utilising an operating system **with a known security vulnerability**.

6%

of organisations encountered **malware installed on a remote device**.

Making the headlines

Spanish prime minister's mobile phone infected by Pegasus spyware, government says

Reuters



MADRID, May 2 (Reuters) - Spanish authorities have detected "Pegasus" spyware in the mobile phones of Prime Minister Pedro Sanchez and Defence Minister Margarita Robles, the government minister for the presidency, Felix Bolanos, said on Monday.

Bolanos told a news conference Sanchez's phone was infected in May 2021 and at least one data leak occurred then. He did not say who could have been spying on the premier or whether foreign or Spanish groups were suspected of being behind it.



A Gift for Paying Your Mobile Bill? Don't Click That Link: It's a Scam

Group texts: Great for scammers, bad for everyone else, as the New Jersey Cybersecurity & Communications Integration Cell is warning T-Mobile customers.



By Nathaniel Mott 18 Apr 2022, 2:37 p.m.



Have you received text messages thanking you for paying your mobile bill, which include a link to a special gift? Don't click; it's a scam, the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) is warning T-Mobile customers.

"Similar to a recent SMiShing campaign targeting Verizon Wireless customers," NJCCIC says, "the message thanks the recipient for paying their bill and includes a malicious link to accept a free gift. The message, however, is sent via group text that includes a number of random recipients and was sent to the targets dozens of times over the course of three days. Customers were unable to block the unwanted messages since they were sent via group text."



LaLiga fined \$280K for soccer app's privacy-violating spy mode

Natasha Lomas @riptari / 11:15 AM GMT+1 • June 12, 2019



Spanish soccer's premier league, LaLiga, has netted itself a €250,000 (~\$280k) fine for privacy violations of Europe's General Data Protection Regulation (GDPR) related to its official app.

As we reported [a year ago](#), users of the LaLiga app were outraged to discover the smartphone software does rather more than show minute-by-minute commentary of football matches — but can use the microphone and GPS of fans' phones to record their surroundings in a bid to identify bars which are unofficially streaming games instead of coughing up for broadcasting rights.

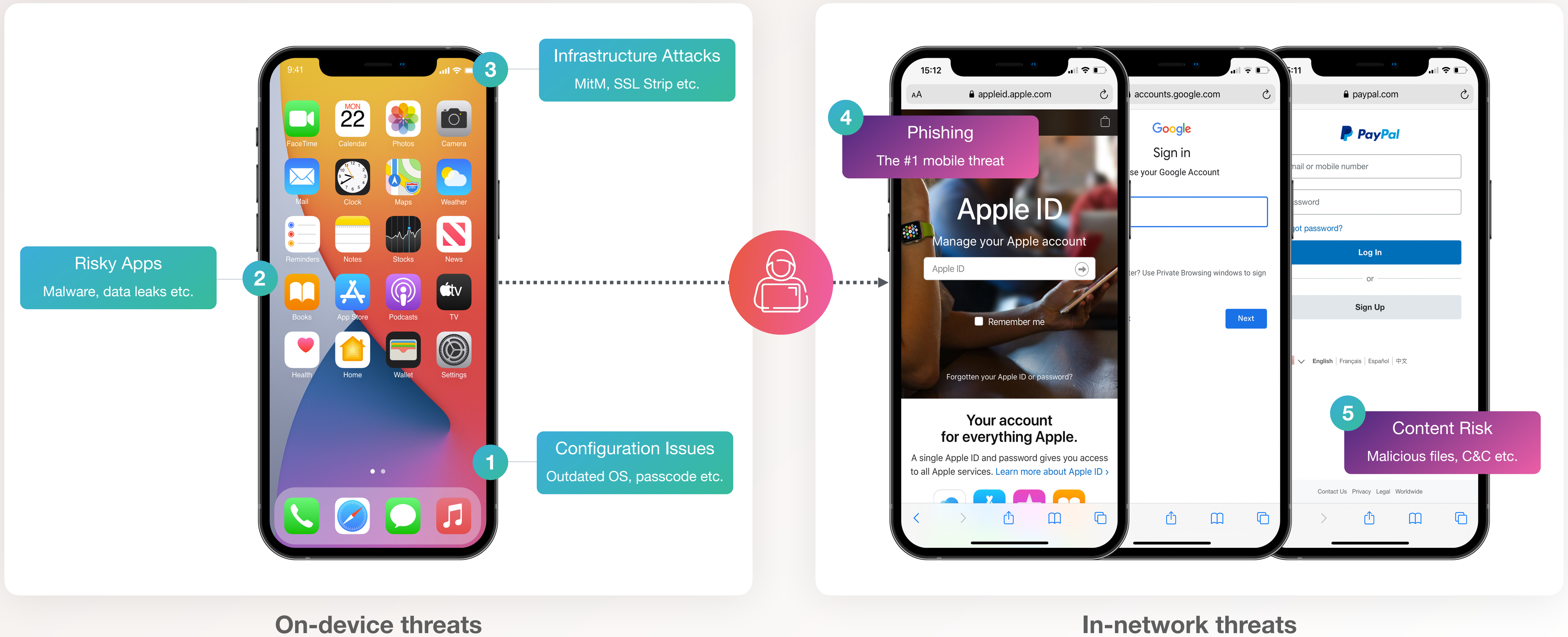
Unwitting fans who hadn't read the tea leaves of opaque app permissions took to social media to vent their anger at finding they'd been co-opted into an unofficial LaLiga piracy police force as the app repurposed their smartphone sensors to rat out their favorite local bars.



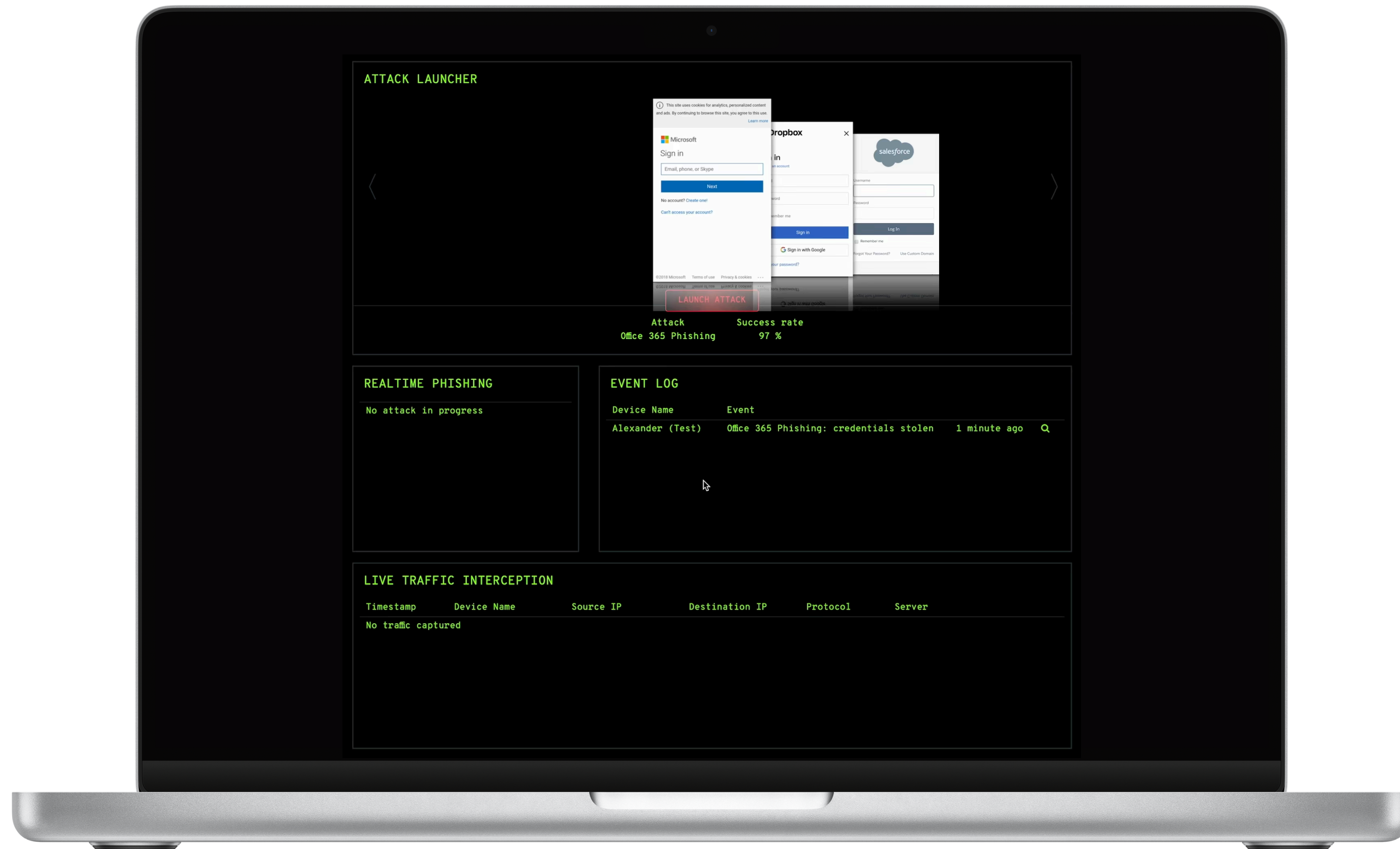
Mobile threats in detail

What sorts of mobile threats are there, and what risks do they pose?

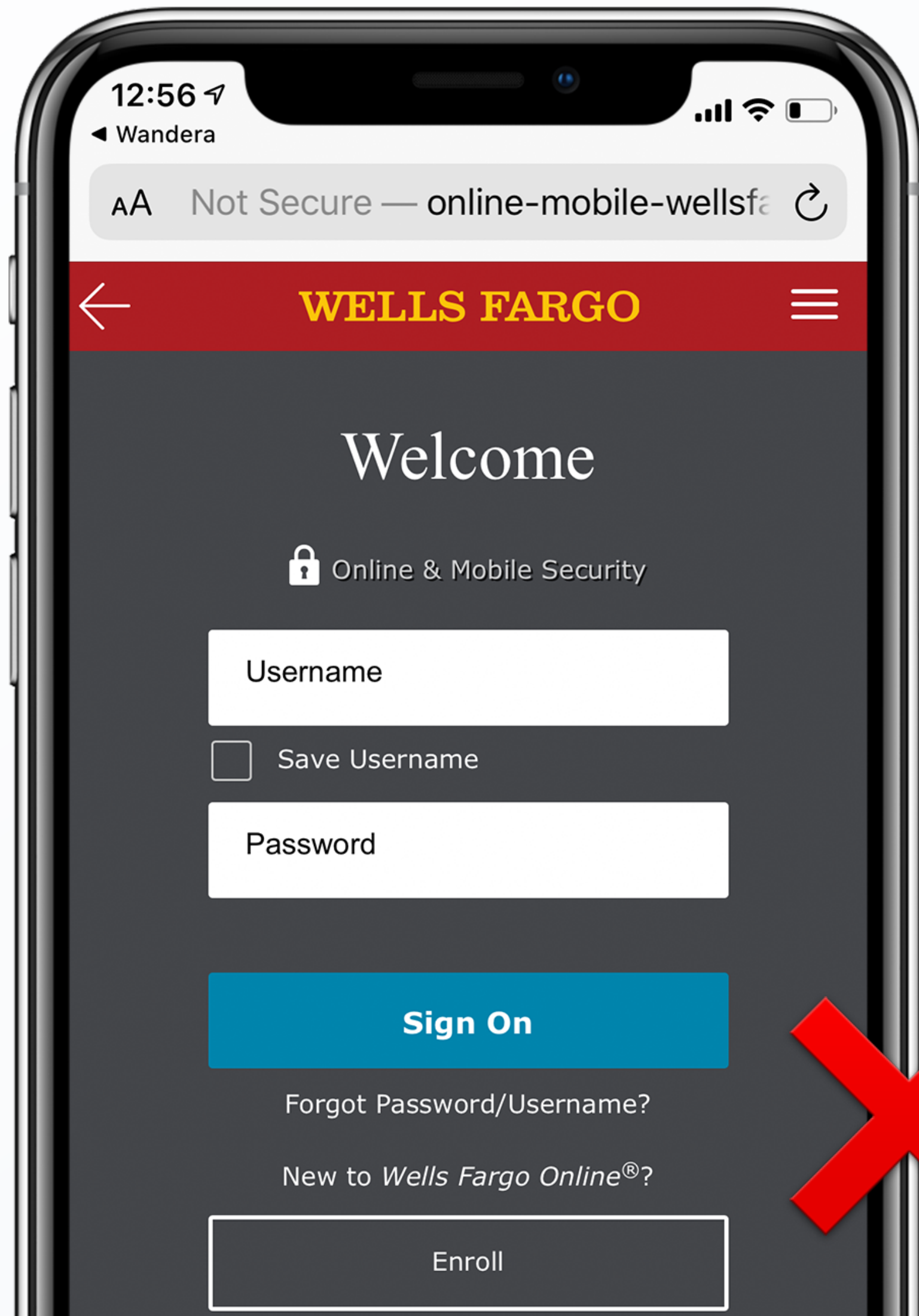
What sorts of mobile threats are there?



The #1 mobile threat vector: Phishing

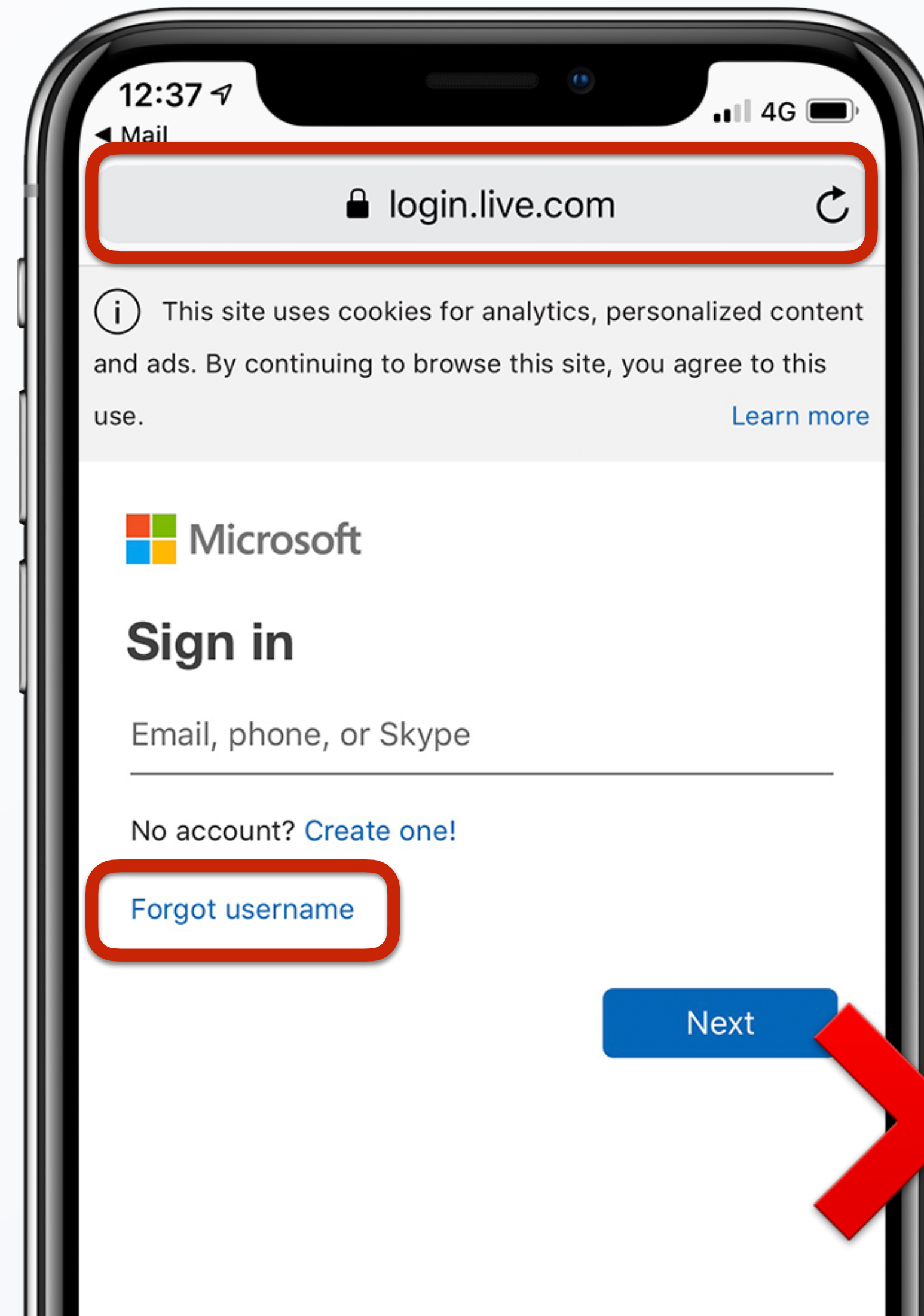
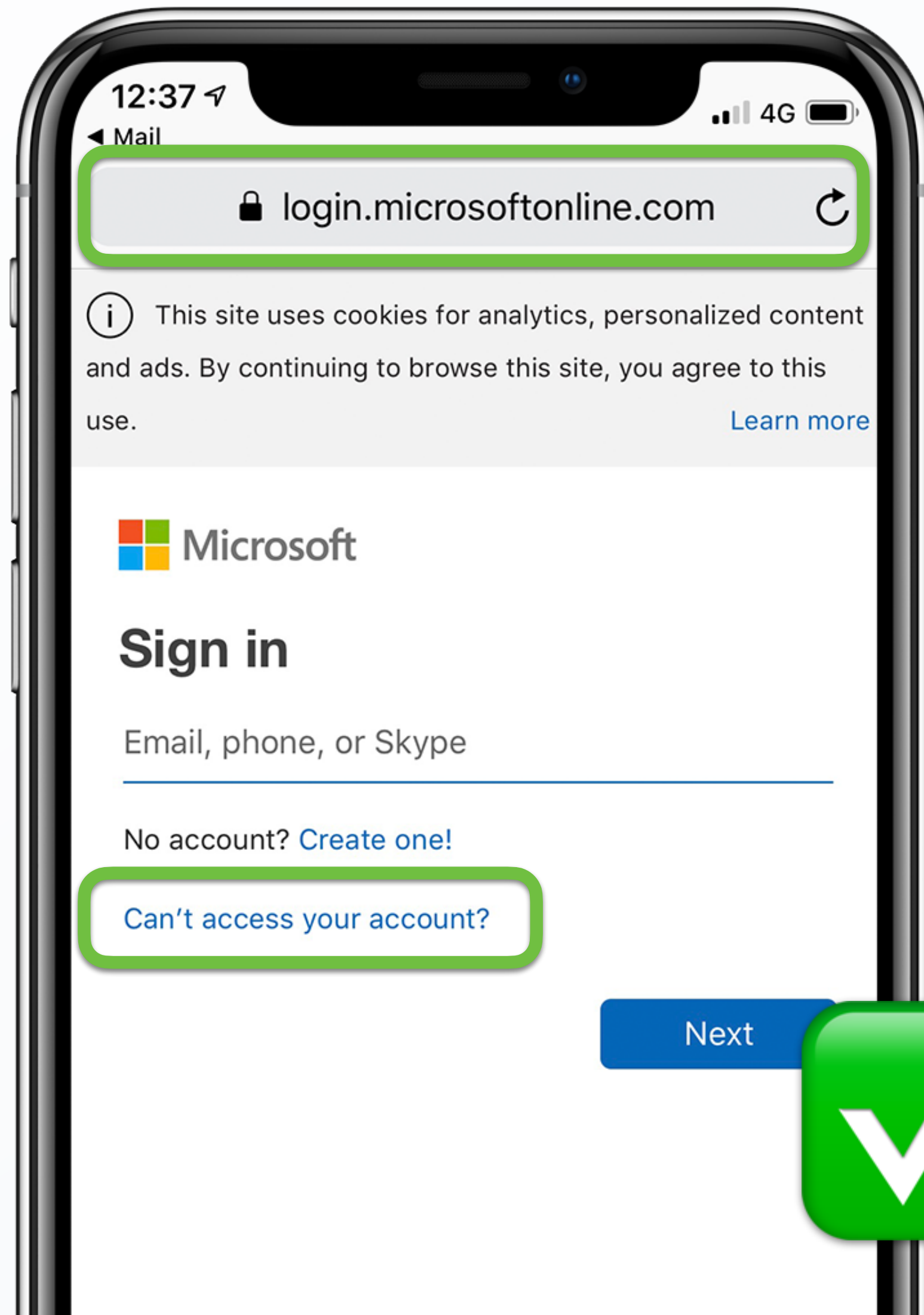


Which is the **real** banking site?



Green padlock icon indicates whether or not the connection is encrypted

Which is the **real** login page?



Different URLs

"Forgot username" -
Different text, same
URL

Near-identical design
and layout

Expect the unexpected: App risk



Mobile apps are fraught with vulnerabilities, even those we know and trust

1 in 4

mobile apps contains at least one high-risk security flaw.

50%

of apps with five to ten million downloads include a security flaw.

3x

Business apps are three times more likely to leak login credentials.

Encryption

Apps without encryption: easy data exfiltration

Permissions

Apps often request excessive permissions access

Vulnerable OSS

Hackers use apps to exploit OS loopholes

Reverse engineering

Apps are disassembled to exploit vulnerabilities

Side-loading

Side-loading of "BETA", or pre-release apps

WhatsApp FREE Vulnerable App

APP IDENTIFIER: net.whatsapp.WhatsApp | DEVELOPER: WhatsApp Inc. | CATEGORY: Communication | IOS APP STORE RATING: 3.08M

App Versions

Version	OS	Devices	App Risk
2.18.80	iOS	3	Medium

App Threat Description CVE-2019-3568

Threat Category: Vulnerable App

Description: This app version is affected by a known vulnerability. The vulnerability allows an attacker to gain access to all data and device functions to which the app has access. The following link provides you with context about this known vulnerability: <https://www.wandera.com/whatsapp-spyware-whats-next/>

App Info View on iOS App Store

Description: WhatsApp Messenger is a FREE messaging app available for iPhone and other smartphones. WhatsApp uses your phone's Internet connection (4G/3G/2G/EDGE or Wi-Fi, as available) to let you message and call friends and family. Switch from SMS to WhatsApp to send and receive messages, calls, photos, videos, and Voice Messages.

RISKY APPS

WeChat 77%

App Risk Score: 77%

Malicious Code Patterns: High

Dangerous Permissions: High

Other Risky App Factors: Anomalous Characteristics, Suspicious Developer Profile, Risky Dynamic Behaviour

REMOVED APPS 3.18K Apps Removed

App	Time in Store	Installs	Risk Score
HUYA LIVE – Ga...	10 days	500K	79%
Truth Social Media	10 days	5K	69%
Guide For Poppy ...	9 days	5K	58%
Rainbow 6 Mobile...	7 days	1K	56%
Wobbly Life Adve...	7 days	1K	52%
Wobbly Tips For ...	8 days	1K	52%
Poppy Huggy Wu...	9 days	1K	52%

How to stay protected

Introducing Jamf Threat Defense, MI:RIAM and the Jamf Trust app



Jamf Threat Defense

Leading **mobile threat defense** for iOS, iPadOS, and Android

Mobile security for all your workers

- ▶ **Detect** configuration vulnerabilities
- ▶ **Protect** against malware & risky apps
- ▶ **Mitigate** malicious infrastructure
- ▶ **Prevent** incoming attacks
- ▶ **Gain** insights through analytics

Introducing MI:RIAM

Mi:riam Analytics RETURN TO RADAR

WHAT MI:RIAM HAS DISCOVERED IN THE PAST 12 MONTHS

- 132,944,981,105 Requests Handled
- 423,072,911 Unique Domains Visited
- 86,625,915 Apps Scanned
- 121,970 Zero-Day Phishing Attacks Identified

Mi:RIAM is the world's most advanced machine learning and mobile threat intelligence engine. It analyses web domains and apps to identify possible threats even before they are encountered on devices. To improve Jamf Security Cloud's threat defence capabilities, Mi:RIAM combs through information from across the Internet every day to discover malware, unknown vulnerabilities and more.

This page contains some of the latest examples of malicious or risky content that has been identified online.

ZERO-DAY PHISHING

Timestamp	URL	Phishing Score
10:35 19 May 2022	www.activate.your.account.paypal.23bn54db.immobiliariaforum.cl	92%
10:35 19 May 2022	activate.your.account.paypal.23bn54db.immobiliariaforum.cl	92%
09:37 19 May 2022	www.paypal.com.mushasconsult.com	91%
06:15 19 May 2022	www.chase-verify-update-account-012212.grenadaexplorer.net	92%
06:15 19 May 2022	chase-verify-update-account-012212.grenadaexplorer.net	91%
04:55 19 May 2022	www.instagram.com-token-764620908782346454685534688872988926r33.yatirimciabi.xyz	94%
04:55 19 May 2022	instagram.com-token-764620908782346454685534688872988926r33.yatirimciabi.xyz	94%
04:47 19 May 2022	stage.elogin.att.com.admin-mcas.ms	90%
04:27 19 May 2022	stage.elogin.att.com.admin-mcas-df.ms	91%
03:20 19 May 2022	verificationprocess-securelogin.com	91%
02:06 19 May 2022	www.applogin.appleid245.apple.com-updateonline.wwsfoxfords.com	97%
02:06 19 May 2022	applogin.appleid245.apple.com-updateonline.wwsfoxfords.com	97%

RISKY APPS REMOVED APPS **3.13K** Apps Removed

10:54

LAST SCANNED

Today, 10:53

SCAN

SECURITY

Require Attention

Jamf

Threat Defense

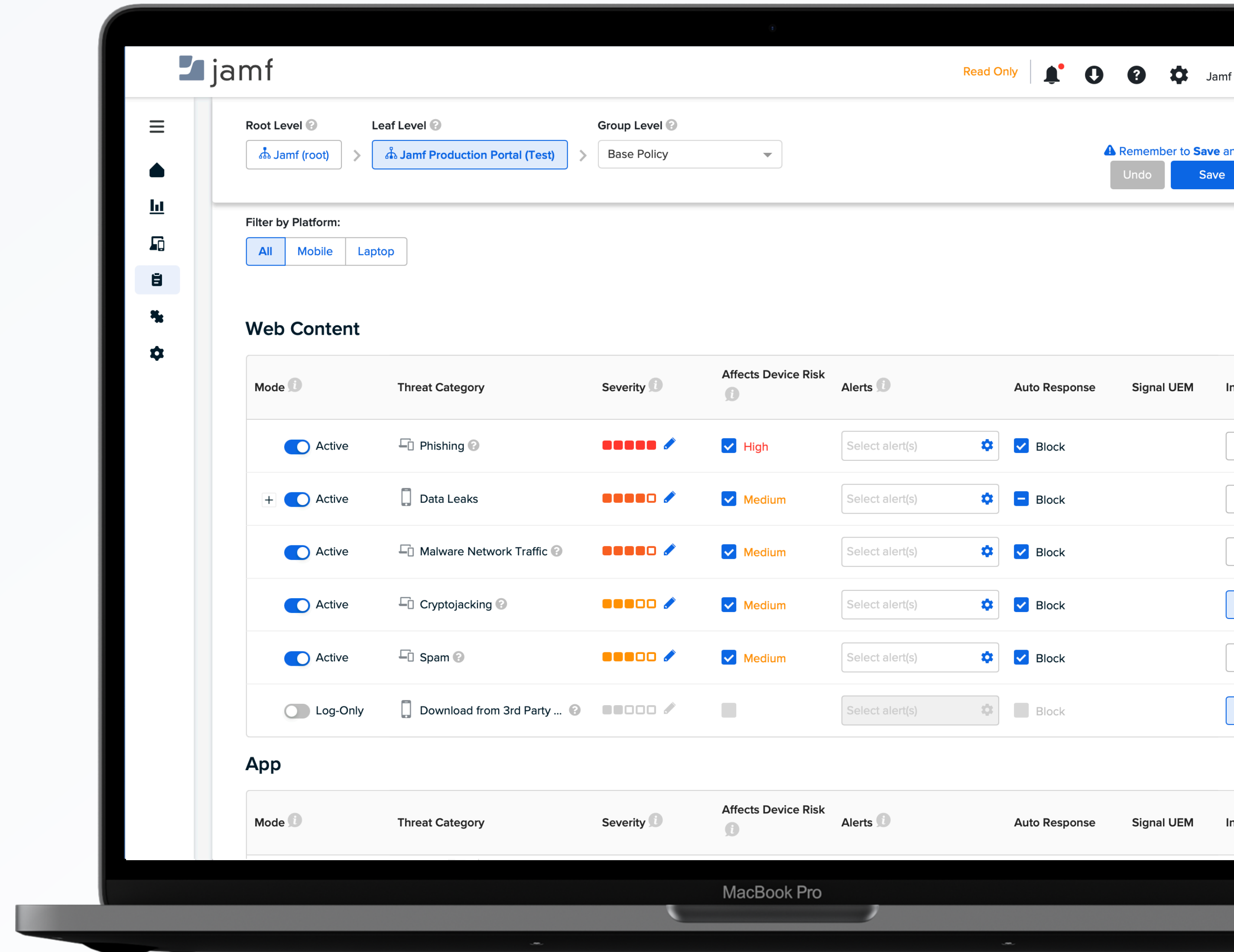
Leading mobile threat defense for iOS, iPadOS, and Android

Detailed analytics

- ▶ Cloud-based, easy-access reporting
- ▶ Comprehensive app vetting

Powerful integrations

- ▶ SIEM, SOAR etc.
- ▶ Zero-touch UEM deployment
- ▶ Conditional access and risk tagging



Jamf Trust

One consistent security experience across platforms

Jamf Threat Defense

Protect end users against malicious domains, phishing, data leaks and other network-based threats

Any ownership model

Whether BYOD, COPE or COBO, empowering all users in a way that protects the business

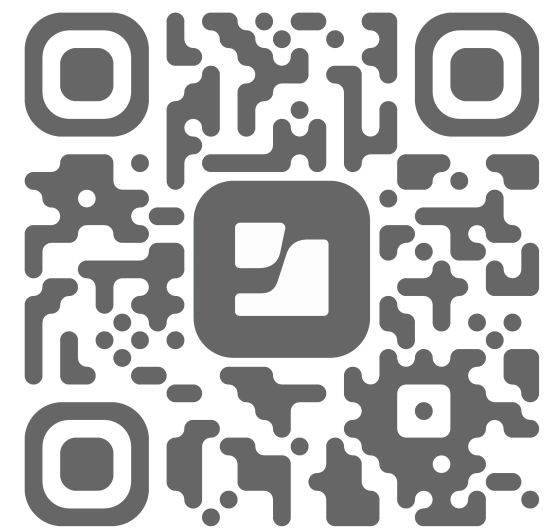


Thank you.



Questions?

Jamf
Threat Labs



Jamf
Threat Defense

