mobileiron
The center of enterprise security

“Proteccion avanzada móvil, el Phishing”

mobileiron THREAT DEFENSE

Joaquin Malo de Molina Muñoz

Iberia Channel Manager
jmmolina@mobileiron.com
630 95 55 25

La tormenta perfecta… para el éxito del hacker

Los ataques moviles han llegado a ser mas creativos…complejos … *sigilosos*

Aun sin brechas?
Las soluciones de MTD son a menudo de prioridad baja

El gasto de seguridad en el endpoint movil una minima fraccion del gasto en seguridad del endopoint tradicional

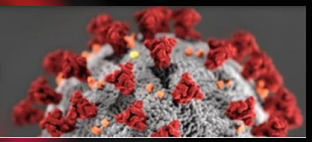
Los Hackers han visto el COVID-19 como una oportunidad enorme

26 MAR 2020 NEWS

#COVID19 Drives Phishing Emails Up 667% in Under a Month

Google blocking 18m coronavirus scam emails every day

FBI Urges Vigilance During COVID-19 Pandemic



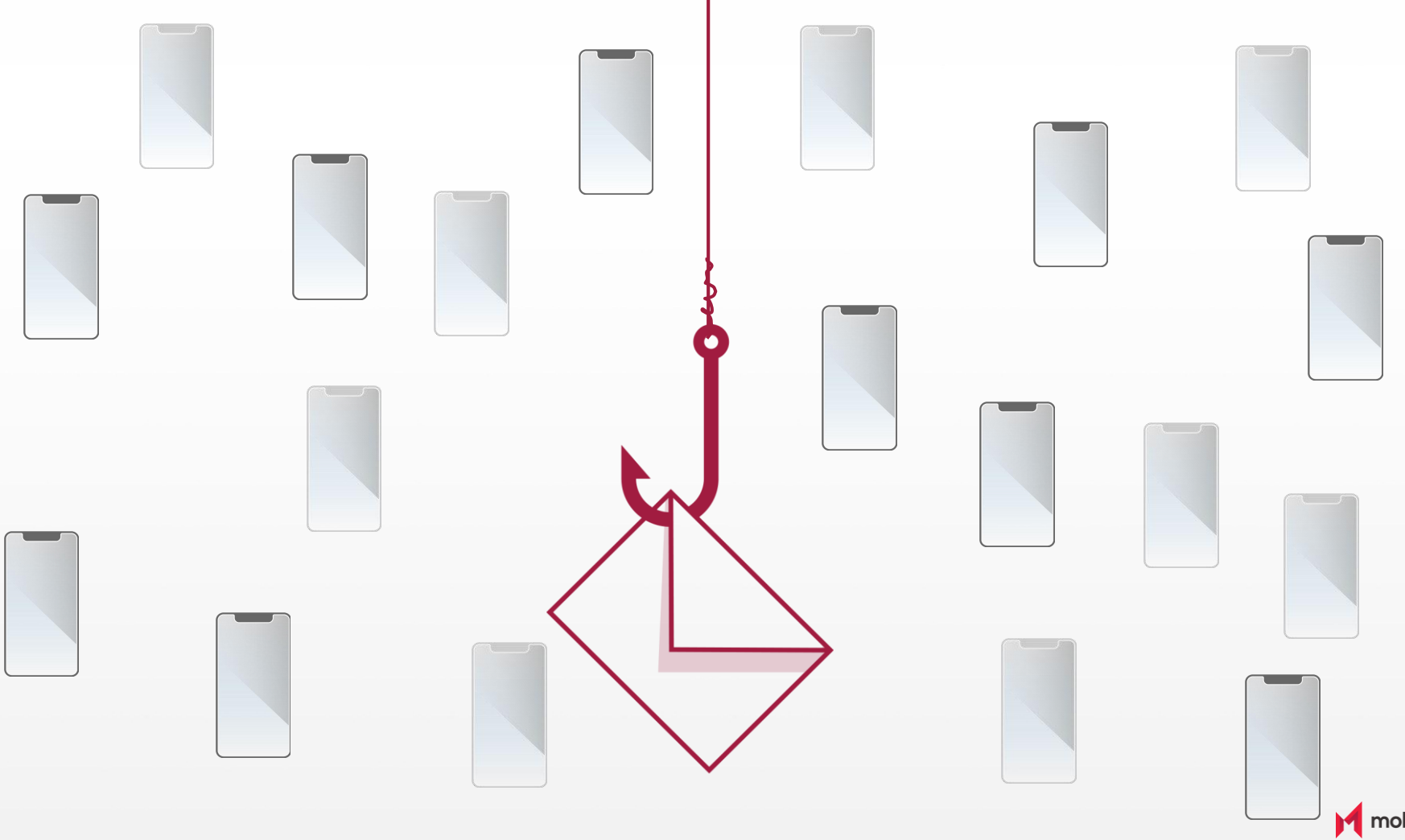
Don't Click! Coronavirus Text and Phone Scams Are Designed to Trick You

Swindlers are taking advantage of the global health crisis, so watch out for email phishing, robocalls and "smishing"—text-message scams sent to your phone.

Ataques Phishing

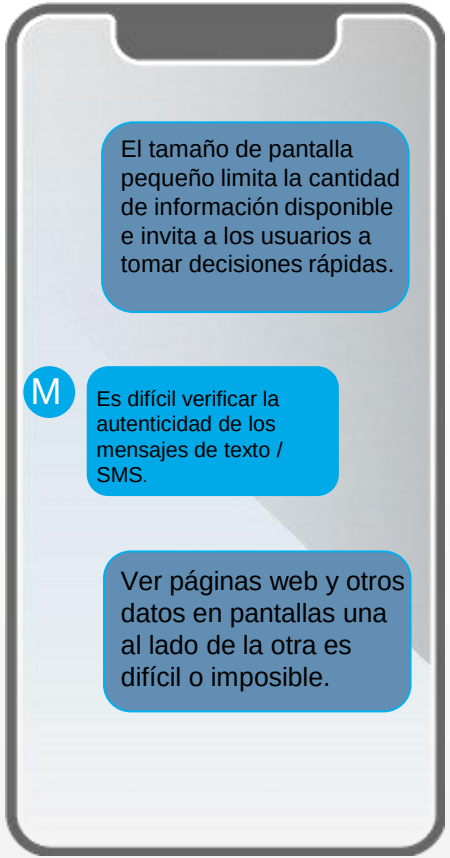
Cuales son estos?

- Ingenieria Social
- Engañar al usuario para que haga clic en un enlace malicioso
- Descarga de malware or exploit kits
- Phishing de credenciales, distribucion de phishing, smishing, whale phishing y vishing



mobileiron

iOS


El tamaño de pantalla pequeño limita la cantidad de información disponible e invita a los usuarios a tomar decisiones rápidas.
M
Es difícil verificar la autenticidad de los mensajes de texto / SMS.
Ver páginas web y otros datos en pantallas una al lado de la otra es difícil o imposible.

¿Qué tienen en común todos estos casos?

EL PAÍS ESPAÑA

ESPIONAJE

WhatsApp confirma el ataque al móvil del presidente del Parlamento catalán

La aplicación de mensajería acredita por primera vez que el teléfono de Roger Torrent fue víctima de un "intento de acceso no autorizado" en 2019

PERIODISTAS Y POLÍTICOS PODRÍAN HABER SIDO ESPIADOS EN LA JOYA DE LA CORONA DE CIUDADANOS

Escrito por TransMurcia | Mar 28, 2019 | ACTUALIDAD, NACIONAL | 0

El error deja a los iPhones vulnerables a los piratas informáticos que roban el contenido del correo electrónico

Una falla en la aplicación de correo incorporada podría permitir a los atacantes leer, modificar o eliminar correos electrónicos, dicen los expertos

El Confidencial

Fallo de ciberseguridad en Palacio: Strava revela las rutas de 'running' en La Zarzuela

Un buen 'zoom' al mapa de calor global publicado por la empresa estadounidense muestra con precisión las rutas que se realizan dentro de la residencia de los reyes de España

BUSINESS INSIDER

La policía detecta intentos de ciberdelincuentes por atacar el sistema informático de hospitales en plena crisis del coronavirus

Alberto R. Aguiar 23 Mar 2020 13:35h.

BUSINESS INSIDER

Alerta por 'phishing': el CNI investiga el hackeo de los móviles de varios ministros y altos cargos del Gobierno

Sofía Sánchez 30 Ago 2020 11:25h.

LA VANGUARDIA | Política

Defensa comunica a la Fiscalía un posible ataque a su red informática interna

• En 2018 se registraron aproximadamente 34.000 ciberincidentes de diverso tipo en entidades del sector público y empresas de interés estratégico

EL PAÍS ESPAÑA

ANDALUCÍA CATALUÑA C. VALENCIANA GALICIA MADRID PAÍS VASCO ÚLTIMAS NOTICIAS

El ataque a los móviles de Torrent y Maragall con un programa espía israelí desata una tormenta política

Interior, Policía y Guardia Civil aseguran que no contrataron los servicios de la empresa NSO

El Confidencial

ATAQUE A LA CIBERSEGURIDAD DEL GOBIERNO

La ministra de Exteriores también fue víctima de 'hackeo' del móvil

Arancha González Laya sufrió el mismo ataque a su teléfono que otros altos cargos y el ministro de Justicia, Juan Carlos Campo

¿Cómo disponer de todos los correos electrónicos?

¿ Es fácil robar un listado de empleados ?

¿Cómo es posible enviar un email infectado a todos los empleados de un hospital?


L6-7 – APPLICATION + PRESENTATION
Data
APPS
AV/Malware (Ransomware, Trojans, Adware, Spyware)
Access Abuse (Unsecured Apps and Privacy Risk)
Repackaged Apps
3rd Party Lib / Back Door
Time Bombs
Download & Execute
USER
Social Engineering
Lack of Security Awareness
False sense of security
BROWSER, EMAIL
Known Browser CVEs
Attachments (PDF, DOC,XLS)
Spear phishing Emails
Session Hijacking
Man In The Browser
Fake SSL Certificates (SSL Decryption)
SSL Stripping
Application
L5 – SESSION
Keys
MULTIMEDIA
Stagefright (24 CVEs)
11+ Threat Vectors (MMS, Browser, Downloads, Email, Facebook App, Gallery, etc.)
Ransomware
CONTAINERS
Unlocked Containers
VPN, Micro VPN
L4 – TRANSPORT
Segment, Datagram
SMS, MMS
Spear phishing SMS
Malicious MMS
Stagefright (24 CVEs)
RECON SCANS
IPv4, IPv6 Scans
TCP, UDP Scans
ARP Scans
L3 – NETWORK
Packet
OS / KERNEL
OS Exploits
Kernel Exploits
Malicious Profiles (iOS)
Network Configuration Attacks (DNS, Proxy, Gateway)
Over The Air (OTA) updates (like Swift Key)
Remote Device Management
Shared Lib Injection
Persistent File System Modifications
WIFI
Rogue AP
ARP MITM
ICMP Redirect
ICMP Double Direct
SSL Striping
Session Hijacking
Fake SSL Certificates
Network
L2 – MAC / DATA LINK
Frame
NFC, BLUETOOTH
NFC Proxy
Malicious Bluetooth
RADIO
Rogue Cell tower / Femtocell
MITM
Location Tracking
L1 – PHSYICAL
Bit
USB
Malicious Chargers
Juice Jacking
Key Loggers
Shared Lib Injection
Unsecured Memory Cards
Device
Play Store
WhatsApp
Inbox
Chrome
Music
Google Maps
Calendar
Messages
Clock
Contacts
Settings
Dropbox

mobileiron
The center of enterprise security

No se QRea todo lo que ve:

Los crecientes riesgos de los códigos QR, *el phishing del Futuro*

mobileiron
The center of enterprise security

El **84 %** de todos los usuarios de móviles han escaneado un código QR alguna vez.*

90,40% en España

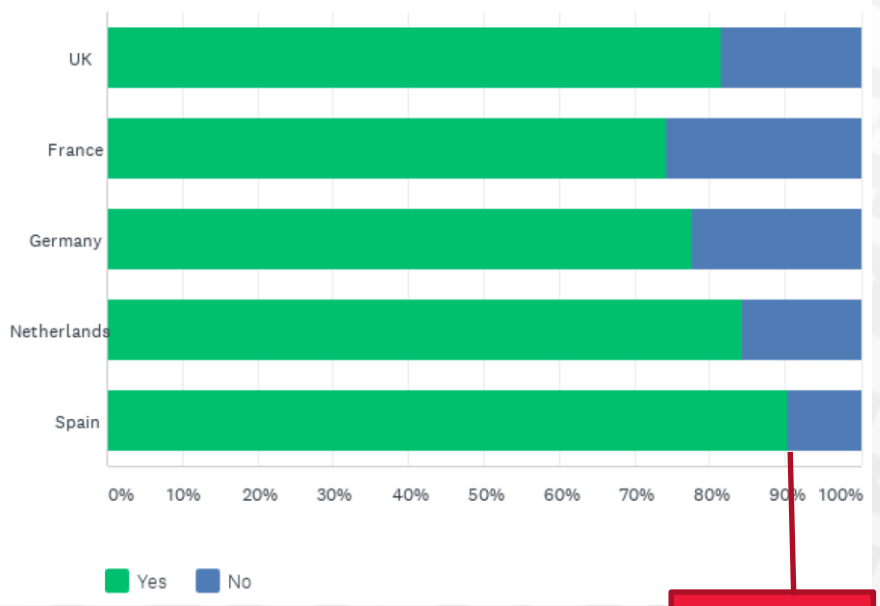
1/3 Más de un tercio de los usuarios de móviles han escaneado un código QR en un restaurante, en una tienda o de un producto de consumo.*

76,9% en España%

* Encuesta realizada por Mobileiron en Europa

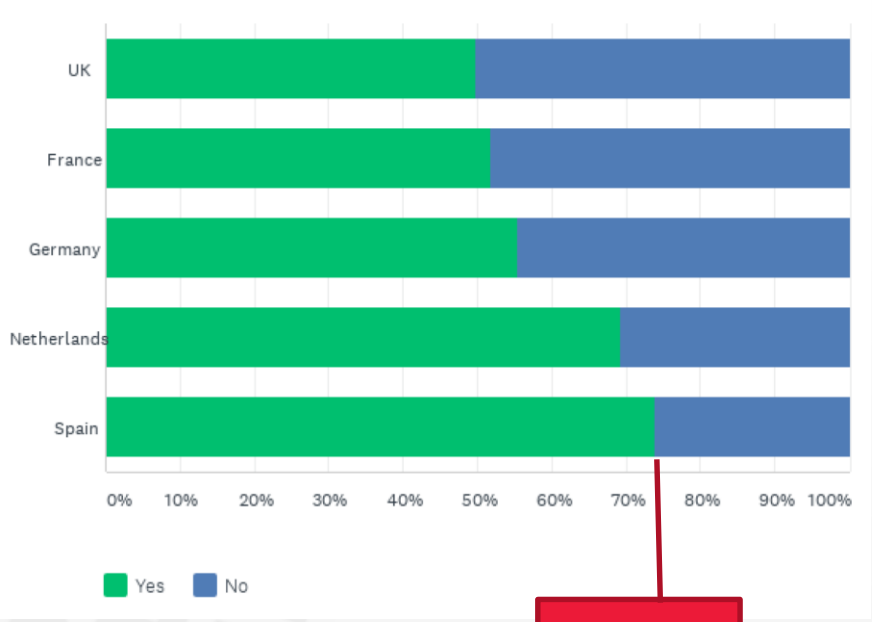
mobileiron
The center of enterprise security

¿Ha escaneado alguna vez un código QR?



90,4 %

¿Crees que utilizarás un código QR como método de pago en un futuro próximo?



73,9 %

* Estos datos y mucho más en nuestro informe “QR Code Sentiment” del 13 de octubre 2020

Los códigos QR: usos

mobileiron
The center of enterprise security

Añadir un contacto:

Pueden añadir automáticamente un contacto nuevo en el teléfono del usuario que podría desencadenar una vulnerabilidad.

Iniciar una llamada telefónica:

Pueden hacer que el teléfono llame a un número y así exponer el número de teléfono a un *hacker*.

Hacer un pago:

Pueden facilitar un pago en cuestión de segundos. Si el código QR es malintencionado, podría permitir a los *hackers* capturar información de pago del usuario.

Escribir un correo electrónico:

Pueden redactar un correo electrónico y rellenar las líneas de destinatario y de asunto.

Enviar un mensaje de texto a alguien:

Pueden crear un mensaje de texto con un destinatario predeterminado.

Revelar la ubicación del usuario:

Pueden enviar la información de geolocalización del usuario a una aplicación.

Abrir una página web:

Pueden enviar el navegador web a una URL predefinida.

Añadir una red Wi-Fi preferida:

Pueden incluir una credencial para la conexión y autenticación automática a una red Wi-Fi. Esto puede introducir una red malintencionada o comprometida en la lista de redes preferidas del dispositivo.

Seguir cuentas de redes sociales:

Pueden hacer que una de las cuentas de redes sociales del usuario siga a otra persona y expongan información personal.

Crear un evento en el calendario:

Pueden poner una reunión en el calendario y potencialmente [illegible] la aplicación los *hackers*.

Cualquiera de estas utilidades van a ser utilizadas para espiar nuestro teléfono y obtener un provecho económico. Extorsión, robo, ….

A nosotros y a la empresa para la que trabajamos

mobileiron
The center of enterprise security

mobileiron
MTD
MobileIron Threat Defense

Seguir cuentas de redes sociales:

Pueden hacer que una de las cuentas de redes sociales del usuario siga una cuenta predefinida y exponga información personal.

Hacer un pago:

Pueden facilitar un pago en cuestión de segundos. Si el código QR es malintencionado, podría permitir a los *hackers* capturar información financiera personal.

Abrir una página web:

Pueden enviar el navegador web a una URL predefinida.

Abrir una página web:

Pueden enviar el navegador web a una URL predefinida.

https://qifi.org/

Mucho más fácil de lo que pensamos

pure JS WiFi QR Code Generator

SSID

SSID

Encryption

WPA/WPA2

Key

key

Hidden

Generate!

Generate! Save! Export! Print!

mobileiron
The center of enterprise security

SSID

La_Wifi_de_un_Hacker

Encryption

WPA/WPA2

Key

NoLoHagas

Hidden

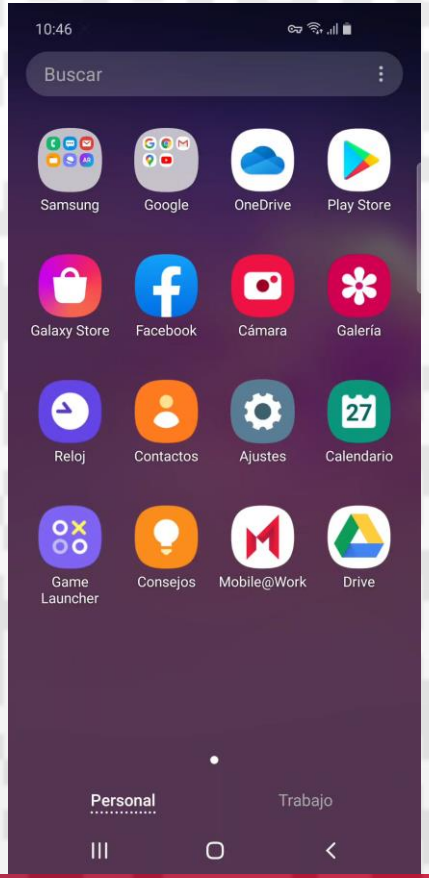
Generate! Save! Export! Print!

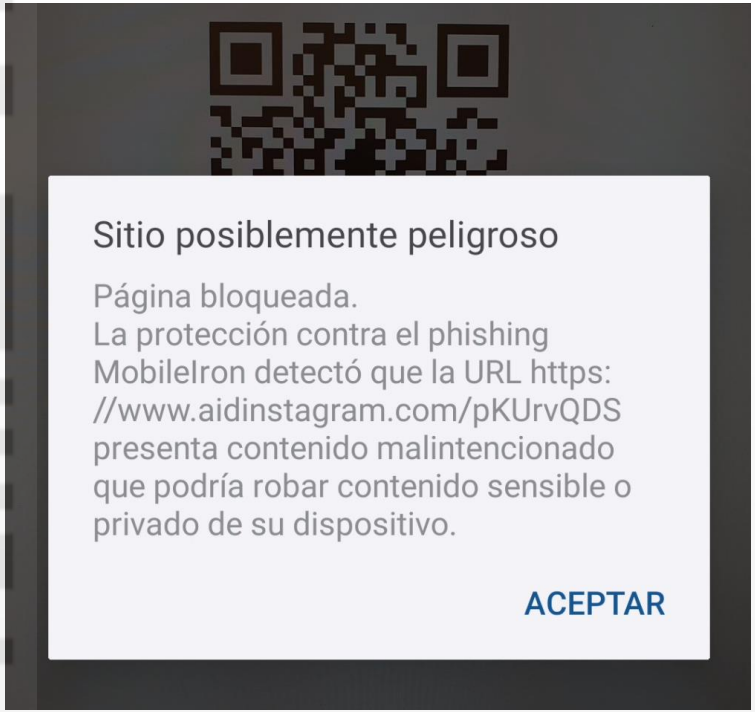
mobileiron
The center of enterprise security

Solución: MTD de Mobileiron

Veamos en directo cómo te ayuda MTD con un par de casos reales

mobileiron
MTD
MobileIron Threat Defense





mobileiron
The center of enterprise security

mobileiron
MTD
MobileIron Threat Defense

Conclusiones sobre QRs

No podemos dejar en manos del usuario
su criterio para saber si el QR es bueno o malo.

Las empresas y organismos
necesitan ciberseguridad todos los móviles

Nuestro diferenciador de proteccion Multivector:

MobileIron Threat Defense (MTD)

mobileiron

MobileIron Threat Defense (MTD) protege y corrige amenazas conocidas y de día cero en dispositivos móviles. No se requiere interacción del usuario para activar MTD, lo que ayuda a impulsar la adopción al 100%.

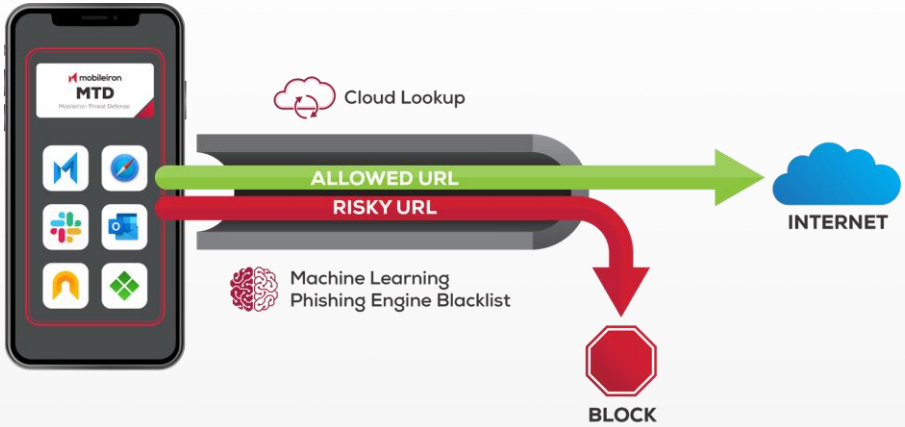
Protección integral contra vectores de ataque

Nuevas capacidades multi-vector anti-phishing & QR

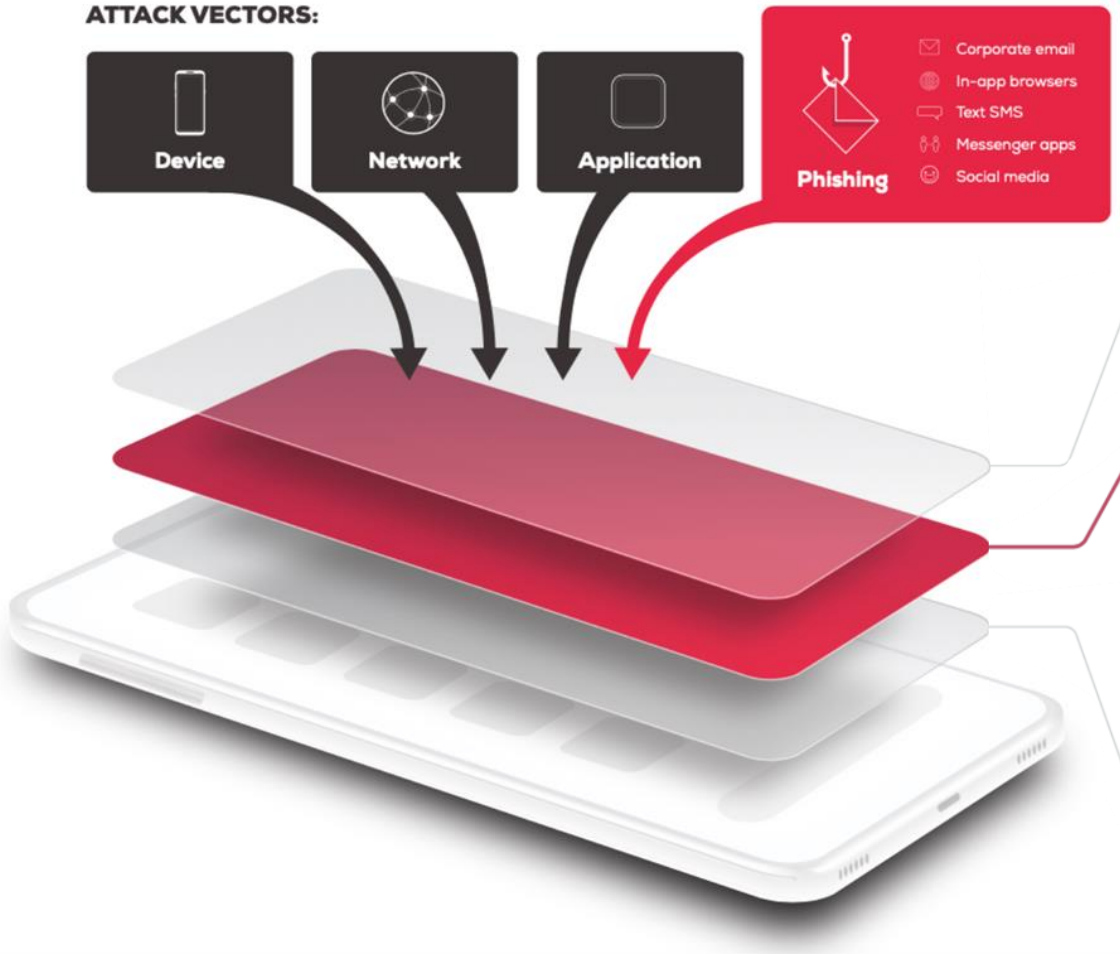
mobileiron

Mejoras anti-phishing claves

Nueva proteccion phishing multi-vector



- Manteniendo e impulsando el 100% de adopción como una realidad
- Machine learning y y búsqueda de URL de suplantación de identidad en el dispositivo, y sin conexión Wi-Fi o de red
- La búsqueda de URL phishing basada en el Cloud mejora la capacidad de detección
- Control y el equilibrio entre "seguridad y privacidad"



mobileiron

MULTI-TIER SECURITY STRATEGY:

mobileiron ZSO

Eliminate passwords

Reduce the risk of data breaches that result from stolen credentials.

mobileiron MTD

On-device detection and remediation for mobile threats

Machine learning-based protection against device-, network-, application-level and phishing attacks (DNAP). No Wi-Fi or cellular connectivity required.

Multi-vector anti-phishing

On-device machine learning and phishing URL lookup can be expanded to include cloud-based lookup for improved effectiveness.

mobileiron UEM

The foundation for the industry's first mobile-centric security platform.

Create and enforce compliance policies to secure your digital workplace.

Proteccion completa phishing movil

Conclusiones clave

Protéjase contra el phishing, el vector de ataque #1

Logre una adopción del usuario del 100%	• Implementación perfecta sin necesidad de acciones del usuario • Las acciones de cumplimiento por niveles ayudan a impulsar y mantener la adopción.
Implementar protección y reparación anti-phishing de varias capas	• Protección contra phishing de varios niveles (native plus VPN-based) • Proteja todo el tráfico de Internet, independientemente de la elección del navegador • Mejora la aplicación de seguridad general y el cumplimiento • Analitica anti-phishing para entender la cobertura empresarial
Control para el equilibrio entre la seguridad y la privacidad del usuario	• Le damos el control para que pueda equilibrar la profundidad en la protección contra el phishing Vs la privacidad del usuario • Elija entre la detección de phishing en el dispositivo (más privacidad del usuario) ... o expanda a la detección en la nube (menos privacidad del usuario)

mobileiron
The center of enterprise security

Joaquin Malo de Molina Muñoz

Iberia Channel Manager
jmmolina@mobileiron.com
630 95 55 25

iOS macOS