MUST-KNOW MOBILE PHISHING FACTS

mobileiron

How prevalent is mobile phishing today?

Hackers are increasingly sending phishing attacks via **text and SMS, social media, productivity applications** and other forms of communication, beyond corporate email.

Mobile phishing attacks are on the rise because hackers are **capitalizing on enterprise security gaps during the COVID-19** pandemic. Hackers know remote employees are leveraging loosely secured mobile devices to access corporate data.

Mobile users are also more likely to fall victim to phishing attacks.

Why are phishing attacks more likely to succeed on mobile devices?

Small screen size limits the amount of available information.

The mobile user interface prompts users to **make fast decisions.**

It's difficult to verify the **authenticity of links** on mobile devices.

What do these attacks look like in the real-world?

COVID-19 text message scams:
Hackers are pretending to be contact tracers and sending fake text messages to alert people that they have been in contact with or near a COVID-19 patient and including malicious links.

LinkedIn spear-phishing campaigns:
Attackers are impersonating HR employees and sending fake job offers with malicious files that contain custom malware and exfiltrate data from victims' devices when opened.

Slack phishing messages:
According to an AT&T AlienLabs report, Slack's Incoming Webhooks, which enable users to post messages from third-party apps to Slack, can be hijacked to send phishing messages and con Slack users into installing malicious apps.

How can organizations defend against these attacks?

MobileIron offers complete mobile phishing protection to detect and remediate phishing attacks across all mobile threat vectors. **Learn more here.**