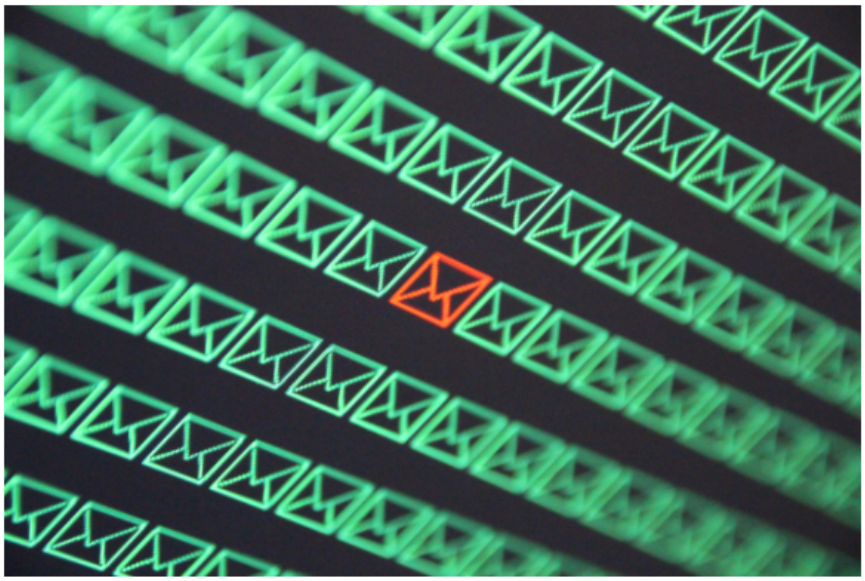
Protecting Your Company From Mobile Phishing Attacks

Dawn Romvari | May 15, 2020



Forms of Mobile Phishing Attacks and How to Protect Your Company

COVID-19 has created a new normal in the world. Employees are working from home — utilizing their mobile devices now more than ever. With this changing landscape comes the opportunity for the increase of cyberattacks like phishing.

What is phishing?

Phishing is a cybercrime that exploits users, through malware or other means, for access to sensitive data.

Categories

Arriver Tips
Business Mileage
CFO Corner
COVID-19
Culture
Finance Focus
HR Hangout
Industry Trends
Internet of Things
IT Insights
Living Cost Intelligence
Managed Mobility Services
Mobile Device Management
Mobile Workforce
Motus News
Oil Check
Remote Work
Risk & Compliance
Technology
Vehicle Programs

Types of mobile phishing?

Email Phishing

Generally, there are two types of emails. One may ask the user to verify personal information using a link. Once clicked, the link will take them to a seemingly legitimate site that is actually fake. The site will then ask them to share information or download something.

Another type of email will have attachments in the form of zip files or word documents. It will request the recipient download the attachment. Once opened, malicious code embedded in those attachments infects their device.

SMS Phishing

As with emails, texts will contain a fraudulent URL disguised as a legitimate site. The site will ask users to input personal information or download an app.

App Phishing

Downloading apps seems harmless on the surface, but users be wary. Legitimate apps feature advertisements. Once the apps are installed, you may get pop-up ads that contain malicious code that will infect your device.

Why are mobile device users more susceptible to phishing tactics?

Users don't pay as close attention to details when using their devices. Mobile screens are smaller. Less information, such as the senders email address and subject lines, is visible.

How do mobile phishing attacks effect companies?

Data Breaches

Once a user provides sensitive information like their username and password, it makes it easier for hackers to breach their other connected devices.

Loss of Revenue

$17,700 is lost every minute due to phishing attacks. Once a hacker has access to your device, your data is vulnerable. They may get access to business processes, customer information or unreleased product and service documents.

Brand Reputation

Companies that have a data breach may suffer irreparable damage to their brand. Customers put their trust in the companies they do business with. Once that trust is gone, the customer is likely to follow.

How do you protect your business from phishing attacks?

The first step in mitigating phishing attacks is educating your employees. Some indicators you may have a phisher on your hands include:

- An email or text message requesting personal information

- An email or text message from an unfamiliar sender with attachments
- Domain names that look legitimate but have additional characters in the URLs that are not associated with the legitimate company
- Generic salutations (although emails that include your first and last shouldn't immediately be ruled out)
- Poor spelling and grammar
- Email subject lines with urgent messages such as 'Your account has been compromised' and 'Urgent action required'

Why do you need a managed mobility solution provider?

The number of smartphone users in the world by the end of 2020 is estimated to be 3.5 billion. Additionally, 94% of malware has been documented to be delivered via email. Phishing attacks account for more than 80% of reported security incidents. The Bring Your Own Device (BYOD) market size is estimated to be valued at over $366 billion by 2022.

With an increasingly mobile workforce, most businesses do not have the systems, staff or expertise necessary to effectively manage today's complex world of mobility. Motus offers end-to-end mobile management solutions to monitor and control devices to protect and safeguard your company against phishing attacks. To learn how you can secure your mobile fleet today, connect with our mobility experts here at Motus!

Connect With Us

The Author

Dawn Romvari

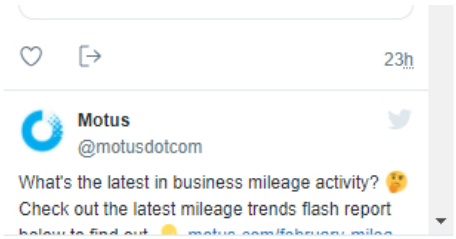
Business and Marketing Development Manager

Read more by Dawn Romvari

malware, mobile device management, mobile phishing attack, security

Loved it?

Share it!



Resources

2018 Fuel Trend Report

Fixed and Variable Rate Program with Motus Mileage Capture App Saves Time and Money

Leveling the Playing Field: Recruit Top Talent With a Better Mileage Reimbursement Program

What's Your Fleet Really Costing You? How to Optimize Your Investment and Cut Costs

Creating Tax Solutions Through Business Vehicle Technology: A Medical Device Company Reduced Its Fica Tax by Almost $500,000