Lookout®

WHITEPAPER

How manufacturers can mitigate mobile phishing risks and accelerate innovation

Understand mobile threat trends so you can better protect mobile devices and cloud applications

Contents

Executive Summary 3

Phishing and malware remain major threats 3

Global pandemic creates new risks 4

Digital safety in a mobile-cloud world 4

Mitigating third-party risk 5

Connected manufacturing spreads risks 5

Protecting intellectual property 5

Compliance requirements are rising 6

Lookout helps manufactures adopt a zero-trust security strategy 6

Lookout mitigates the mobile threat for manufacturers 6

Key takeaways 7

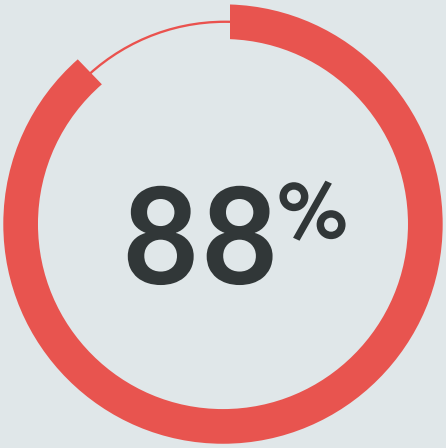
About Lookout 7

Executive Summary

Manufacturers are transforming the way they produce and deliver goods - moving toward industrial automation and the flexible factory. This transformation, known as Industry 4.0, puts pressure on mobile devices and cloud solutions as manufacturers realign themselves to make sure they can effectively transition their work from the design studio to the shop floor. Mobile apps, data analytics, and internet of things (IoT) devices offer an unprecedented opportunity to create innovative new products, drive revenue, and increase operational efficiency.

Cybersecurity risk cannot be underestimated. 50% of manufacturing executives indicated they lack confidence that their company's assets are protected from external threats, according to Deloitte[1]. Every smartphone and tablet should be treated as a potential source of threats. Whether it is in the hands of an engineer, a business development executive, or the HVAC service person. Adopting a security solution that adheres to a zero-trust model, where the health of all mobile devices are monitored in real-time, will ensure your organization's data is secure.

This whitepaper provides an overview of key mobile threat trends faced by manufacturers and their potential impact on your business; from the inherent risks of cloud apps to the ongoing need to protect intellectual property and maintain industry compliance. Finally, we'll find use-cases highlighting how other manufacturers are protecting their business against the latest phishing and other mobile threats.



of credential theft is achieved by phishing[1]

Phishing and malware remain major threats

People are busy, device screens are small. We work quickly, instinctively, and often distractedly on our mobile devices. So it's no surprise that phishing is the primary way malicious actors trick people into downloading malware. Attackers are clever about targeting and tricking individuals, especially executives, sales, and finance, into downloading malware or inadvertently granting them access to corporate resources.

European manufacturers face phishing threats at double the rate of their global peers. In 4Q2019, Lookout measured that 14% of mobile devices in the manufacturing industry encountered a phishing link, compared to only six percent for manufacturers in other regions. See the State of Mobile Phishing[2] report for more detail.

There are many real-world examples of ways phishing and malware can exploit mobile device vulnerabilities to steal data, change the configuration of the device, lock out the user until ransom is paid up, or brick the device. Malware can allow the attacker to jump over to the operational technology (OT) network, spreading disruption and destruction.

WhatsApp can now be hacked to change the text of a message and identity of a sender, we learned from an attack that tricked one of the most prominent tech executives. Shady malware can slip onto Androids[3] directly from the Google Play store. Pegasus spyware can bypass device security without a user's knowledge action and steal information like contacts, location, and passwords. The surveillanceware Monokle uses advanced data exfiltration techniques and can install an attacker-specified certificate to the trusted certificate store on an Android device to facilitate a man-in-the-middle attack.

[1] "Cyber risk in Advanced Manufacturing; Getting ahead of cyber risk." Deloitte and Touche LLP, https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

[2,3] Andy Greenberg. "How Spies Snuck Malware into the Google Play Store – Again and Again". Wired. 28 April 2020, https://www.wired.com/story/phantom-lance-google-play-malware-apt32/

Permanent shift to remote work creates new risks

Cyberattackers are taking advantage of the confusion during the coronavirus crisis and security incidents are growing as organizations shift to remote working. In fact, 23 percent of organizations said cybersecurity incidents have increased since transitioning to remote work, according to (ISC2).

As remote work becomes our "new" normal, manufacturers must ensure their workers are protected against phishing, malware, and other mobile attacks, no matter where they are.

In March 2020, Lookout identified an Android app called "corona live 1.1." Upon launch, the app informs the user that it doesn't require special access privileges, then goes on to request access to phones, media, files, device location and permission to take pictures and record video. The app is a trojanized version of the legitimate "corona virus" app, which provides an interface to the data used in the John Hopkins coronavirus tracker.

Security leaders at manufacturers have long been concerned about the risk of public Wi-Fi hotspots, but now remote work is a business continuity imperative. Many employees underestimate the risk.

> Prior to the pandemic, **77 percent of manufacturing workers said they personally used public Wi-Fi for work**, even though it was prohibited by policy at 42 percent of their organizations.
>
> 2020 Verizon Mobile Security Index[4]

Manufacturing leaders have also been concerned about the digital protection of their people, devices, and data traveling to Asia. One Lookout customer told us that after 10 employees travelled to Asia, more than 100 incidents, including malware, where found on those devices. Some companies have even implemented a one-phone-per-trip policy, and when an employee returns from a trip to Asia, their phone is thrown away.

A recent Lookout mobile threat discovery of four interconnected surveillanceware tools originating in China, further exemplifies the cybersecurity risk that China can present. The primary aim of the malware is to gather and exfiltrate personal user data to attacker-operated command-and-control servers. Activity across these tools dates back to 2013.

Digital safety in a cloud-driven world

Manufacturers have embraced software-as-a-service (SaaS) for productivity and collaboration, customer management, human resources, finance, manufacturing execution and supply chain. The benefits are many. With cloud tools, employees, customers and partners can collaborate more effectively. Mobile apps and devices improve planning and control and provide greater transparency on the shop floor. Machinery operators can add descriptions, pictures, and videos on their mobile devices, reducing paperwork. Workers use self-learning resources for safety training and to acquire new skills.

At the same time, credential abuse is the top attack vector for SaaS and cloud apps. In fact, 40 percent of enterprises say their Microsoft Office 365 account credentials have been compromised, according to Osterman Research[5], with incidents more common in the UK.

[4] Verizon. 2020 VErizon Mobile Security Index, 2020.

[5] Osterman Research Survey Report. "Office 365 Email Security in the Enterprise: 2019 Benchmarking Survey." Cyren. July 2019

Mitigating third-party risk

An expansive supply chain puts manufacturers at greater third-party risk. Manufacturers rely on a web of external workers, contractors, and service partners to maintain equipment on the factory floor, clean machinery, package products, manage waste, ensure worker safety, and much more.

Technicians from one vendor may share the same device among the team as they access applications in the cloud. They may access a manufacturer's email or HR system or take training courses from these third-party devices. Some vendors might have mobile device management (MDM) installed to adhere to the manufacturer's security policies.

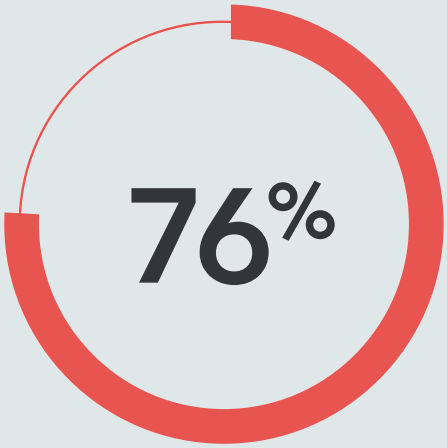
Connected manufacturing spreads risks

To remain competitive, manufacturers are investing in intellectual property and new technologies like digital twins. Digitizing manufacturing, inventory tracking, operations, and maintenance increases agility and efficiency, with less production downtime and a greater nimbleness.

While the connectedness of a smart factory accelerates innovation in products, manufacturing and supply chain management, it also creates cybersecurity risk. The manufacturing floor is no longer air-gapped from the corporate IT network. Threats from mobile devices can spread from the corporate IT network to the OT network. Industrial control systems are now vulnerable. IoT strategies are enabling new ways to drive customer service and business efficiency, but the security of many IoT devices is not field-proven.

Protecting intellectual property

Protecting intellectual property and trade secrets is paramount. Automotive manufacturers are building safer cars that can reduce accidents. Pharmaceutical companies invest billions in drug development, and must protect information from their proprietary research and clinical trials. Data from research labs is more valuable than ever in the global race to develop accurate tests and vaccines for coronavirus. In aerospace and defense, the stakes for protecting innovation is not just a matter of competitive advantage but also national security.



of manufacturers have a smart factory initiative
– CapGemini[6]

87 percent of manufacturers are concerned about competitors stealing their trade secrets or intellectual property.

2020 Verizon Mobile Security Index

[6] Rossman, Markus. "Smart Factories: How can manufacturers realize the potential of digital industrial revolution.", CapGemini, May 15, 2017.

Compliance requirements are rising

Europeans place a high value on personal privacy. The EU's General Data Protection Regulation (GDPR or DSGVO in Germany) has created stringent breach notification requirements and stiff fines on companies that do not adequately protect personal data. In 2019, 27 companies were fined at least €100,000, according to a GDPR fine tracker[6].

Organizations have been working to operationalize these new legal requirements, and those who fall to data breaches face serious financial penalties. Manufacturers have increased audit frequency to ensure they remain in compliance, which consequently calls for new ways to streamline security reporting.

Manufacturers should adopt a zero-trust strategy

Mobile security helps manufacturers adopt a zero-rust approach. Here at Lookout, we continuously monitor device health and protect users and enterprise data from the latest phishing, app, device, and network threats. In short, all devices are guilty until proven innocent. And with unparalleled visibility into the health, identity, and context of the apps, device, network, and corporate data, we continuously adapt our machine learning models to detect emerging threats with high fidelity. Lookout creates a fingerprint of each mobile device and compares it with data from nearly 200 million mobile devices. iOS and Android device health, whether company-owned or personal, is validated during authentication. Lookout then provides continuously validated, conditional access to corporate data.

Lookout mitigates mobile threat for manufacturers

Lookout provides comprehensive protection against the entire spectrum of mobile risk, which includes threats, vulnerabilities, and configuration risks across the four primary threat vectors - phishing, app, device, and network threats.

[6] Coreview. "Major GDPR Fine Tracker - An Up-To-Date List of Enforcement Actions". Coreview Blog, July 13, 2020.

Mobile phishing

Lookout detects and tracks 10,000 active phishing sites every day. We can monitor phishing attacks coming from all sources, including SMS, social media apps and internet-based messaging apps. Our AI-driven platform proactively determines the reputation of internet sites and detects phishing kits as they are being built, long before any user is targeted or an attack is executed.

App threats

Lookout has analyzed more than 100 million applications, which provides us with visibility into risks such as trojans and spyware. As a member of the Google App Security Alliance, Lookout also scans every app in the Google Play Store and reports malicious apps for removal.

Device risks

Lookout also protects against device-based risks that occur when the built-in security of the operating system has been bypassed. Lookout can identify behavioral anomalies, rooting or jailbreaking, out-of-date operating systems, and device configuration risks.

Network risks

Lookout protects against network risks, which is especially important as so many more employees work from home and will continue to use public Wi-Fi hotspots. Lookout analyzes network connections and can accurately identify man-in-the-middle attacks, host certificate hijacking, hijacked SSL traffic, and TLS protocol downgrades.

Enforce data privacy policies and protect employee information

Lookout helps companies maintain their data privacy policies, both internal and industry regulations and laws. If regulated content is being accessed and shared improperly, the security team will be promptly notified. If a device exceeds an acceptable level of risk, we will notify the employee and the IT manager and can log the employee out of corporate resources. With a data-driven platform, we also do not inspect the content we protect, respecting the privacy of your organization and your employees.

Key takeaways

1. Phishing and malware remain the primary threat vectors targeting the manufacturing industry.
2. A zero-trust security strategy is more critical than ever as threats evolve to take advantage of an expanded remote workforce.
3. Mobile threat defense is a necessary component for securing a mobile workforce that is increasingly targeted by phishing, application, device, and network attacks.

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play.

The broad adoption of smartphones and tablets have created new and endless ways for cybercriminals to convince you to willingly use your mobile device for their unlawful gain. The most common start of a cyberattack is a phishing link and mobile devices have enabled new ways to send them to you. Phishing risks no longer simply hide in email, but in messaging, social media, and even dating apps. Because we use these devices for both, protecting against phishing is critical for our personal and professional lives.

Lookout enables consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk. As a result, Lookout delivers modern endpoint security with the most comprehensive protection from device, network, app and phishing threats without prying into your data.

To learn more, visit lookout.com.