Mobile Security awareness programme

why should you invest in a Mobile Security awareness programme?

You'll learn about mobile security vulnerabilities and threats in this in-depth exploration of mobile security in the company. Investigate the ways in which attackers might exploit mobile devices to do harm to businesses. Using a wide range of mobile, smart, and platform devices (including iOS [iPhone and iPad] and Android), we demonstrate a wide range of mobile security challenges, technical problems with mobile platforms, remediation tactics, security policies, and remedies.

How mobile security works?

The next generation of cybercriminals will be defeated, but only if we invest in mobile security. There isn't just one kind of mobile security. You may rely on some of the safeguards that were included into your gadget.

The iPhone, for instance, has an inbuilt Auto lock function that locks the screen after a certain amount of time. if the device hasn't been used. Strong encryption standards for data travelling over cellular networks are only one example of the additional mobile security measures embedded into the network.

A well-informed user, on the other hand, who takes precautions to prevent the disclosure of private information by not installing potentially malicious software or visiting malicious websites, may be more effective than any mobile security gadget

What are the types of mobile security ?

There are four different types of mobile security models used by vendors.

Traditional signature file antivirus approach.

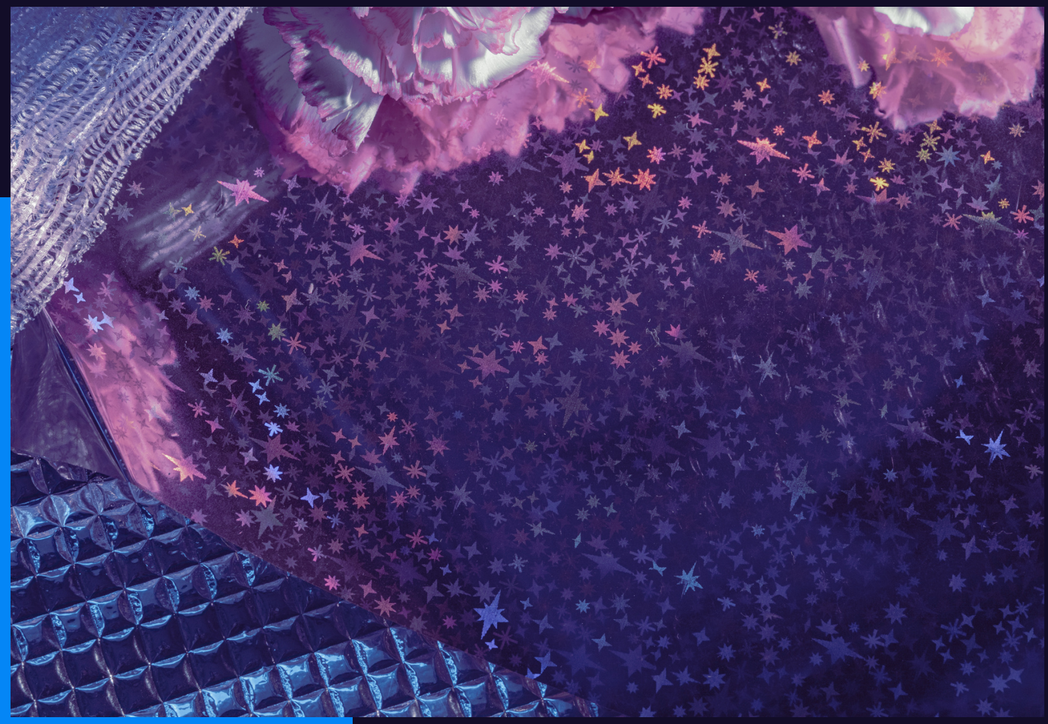
Hybrid-AI cloud security.

Intermediary cloud approach.

Mobile behavioral analysis.

How to protect yourself from mobile security threats?

- Keep your software updated.
- Choose mobile security.
- Install a firewall.
- Always use a passcode on your phone.
- Download apps from official app stores.
- Always read the end-user agreement.



WHAT ARE THE MOBILE DEVICE SECURITY BEST PRACTICES?

1. Enable user authentication
2. Always run updates
3. Avoid public wifi
4. Use a password manager
5. Enable remote lock
6. Cloud backups
7. Use MDM/MAM

WHAT ARE THE SECURITY THREATS TO MOBILE DEVICE?

1. Malicious Apps and Websites
2. Mobile Ransomware
3. Phishing
4. Man-in-the-Middle (MitM) Attacks
5. Advanced Jailbreaking and Rooting Techniques
6. Device and OS exploits

SMART PHONE SECURITY THREATS

Downloadable Applications Threats:

- Malware
- Spyware
- Privacy
- Zero Day Vulnerabilities

General Cyber Security Threats:

- Phishing
- Social Engineering
- Drive By Downloads
- Browser Flaws
- OS Flaws
- Data Storage

Network and WiFi Security Threats:

- Network Exploits
- WiFi Sniffing
- Cross-Platform Attacks
- BOYD

Physical Threats:

- Loss/Theft

RISKS FOR MOBILE DEVICES

Offline Risks	Online Risks
Theft	Data Harvests
NFC Swiping	Man in the Middle
Proximity Hacking	Trojans & Viruses
	Spying & Snooping
	Metadata Collection