Q.1. what is smishing and how it defers from vishing?

Sol:- Smishing is type of social engineering attack that uses SMS (short message service) or text messages to trick individuals into revealing sensitive informal or performing certain action. It is a form of phishing that uses mobile devices as the attack vector.

→ Smishing uses text message (SMS) to trick you but vishing uses voice calls to trick you.

→ In smishing scammers sends fake messages that appear to be form a legitimate source, while in vishing scammers call you, claiming to be from a legitimate source.

→ In smishing they asks you to provide info or pay money.

Q.2. Compare mobile computing Vs wireless computing?

Sol^n:- → Mobile computing emphasizes device portability, while wireless computing emphasizes wireless connectivity.

→ Mobile computing can occur with or without wireless connectivity while wireless computing require wireless technology.

→ Mobile computating focuses on accessing and processing data on the go, while wireless computing focuses on transmitting and receiving data wirelessly.

→ Example of mobile computing are using a smarthphone to check email, browsing the internet on a tablet, while example of wireless computing are connectivity to a WI-FI network transferring files via Bluetooth.

3. Examine about the Mobility and its trends?

Ans:- Mobility refers to the ability to move freely and easily from one place to another. In the content of technology, mobility trends refers to the shifting patterns and advancement of in mobile devices, networks and applications.

⇒ Mobility Trends :-

1. Increased Smartphone adoption.
2. 5G Network.
3. Mobile first approach
4. Remote work and virtual teams.
5. Augmented and virtual Reality.
6. Artificial Intelligence (AI) and machine learning.
7. Internet of Things (IOT).
8. Mobile Payment and commerce.
9. Security and privacy.

Discuss Organization measure for handling the mobile devices?

Ans:- 1) Mobile device Management (MDM) :-

Implement MDM solutions to manage and secure mobile devices, including mobile applications management device encryption and remote wipe capablities.

2) Mobile Threat Defence (MTD) Solutions:-

Use MTD solution to detect and present mobile threats including malware, phishing and other attacks.

3) Mobile Security Information and Event Management (SIEM) System:-

Implement mobile SIEM system to monitor and analize mobile device activity, detecting potential security threats.

4) Mobile device vulnerability management:-

Regularly assess and patch mobile device vulnerability to present explanation.

5) Mobile data protection:-

Implement measures to protect mobile data, including encryption, secure storage and data loss preventions.

6) Mobile device security training:-

Provide regular security training to mobile device users.

7) Continuous Monitoring:-

Continuously monitor for security mobile device and app for security threats and vulnerabilities.

5. Summarize the proliferation (growth) of mobile and wireless devices.

Ans:- The proliferation of mobile and wireless devices has led to -

1) Increased Connectivity:- More people and devices are connected to the internet and each other.

2) Explosive Growth :- The number of mobile devices and wireless connections has grown exponentially.

3) New Applications :- Mobile devices have enabled new applications and services such as mobile payment and streaming.

4) Changing Behaviour :- Mobile device have changed how people communicate, work and access information

5) Increased dependary :- People relay heavily on mobile devices for daily activities.

6) Security Concerns :- The growth of mobile devices has increased security risks and threats.

Q.6. Examine the credit card frauds in mobile and wireless devices?

Sol^n:- 1) Phishing Attacks :-

Scammers tricks users into revealing card details through fake email, text or apps.

2) Mobile Malware :-

Malicious apps or software, steal cards information or intercept payment data.

3) Card skimming :-

Devices attacks attached to card readers or ATMs steal and card information.

4) Identify theft :-

Criminal use personal info. to open new credit accounts or make fraudulent purchase.

5) Mobile device theft :- Stolen devices are used for fraudulent transaction or to access card info.

6) Public WI-FI Interception :-

Hackers intercept card info. transmitted over unsecured public WI-FI networks.

7) SMS based fraud :-

Scammers use texts msg to trick users into revealings card details or installing malware.

Q.7. Interference about the Registry settings for mobile devices in details?

Sol^n:- Register setting for mobile devices refer to the configurations settings stored in the devices registry that control various aspects of the device's behaviour and punctionaity. Here are some inferences about registry settings for mobile devices.

1) Application Management :-

Registry setting manage applications, installations, updates and permission, ensuring that apps run smoothly and security.

2) Security policies:- Register settings manage configure network settings such as APN setting, PNS setting and network proxy settings.

3) Network settings:- Register settings enforce security policies including password policies device lock settings and network proxy settings.

4) Device performance:- Register setting optimize device performance such as language setting, font-size, and accessibility options.

5) Hardware settings:- Registry settings control hardware including camera setting, audio setting and sensor setting.

6) Trouble Shooting:- Register setting aid in trouble shootings by providing error logs, crash dumps and diagnostic information.

Q.8. Discuss the popular types of attacks against mobile networks. Discuss the common attacks on bluetooth devices?

Soln:- Popular types of attacks against mobile networks -

1) Eaves Dropping :- Intercepting mobile phone conversation and data transmissions.

2) Stingray :- Using a fake call tower to track mobile devices.

3) Man in the Middle (MITM) :- Incepting and altering communication b/w two parties.

4) Denial of service :- Overwhelming a network with traffic to make it unavailable.

5) Malware :- Inflecting mobile devices with malicious software.

6) Phising :- Tricking users into revealing sensitive information.

→ Common attack on Bluetooth devices:-

1) BlueSniffing :- Detecting and exploiting vulnerabilities in bluetooth devices.

2) Bleue jacking :- Sending unwanted message or files to a Bluetooth device.

3) Bluesnasfing :- Unauthorized access to bluetooth device data.

4) Device Spoofing :- Impersonality a trusted bluetooth device.

5) Malware :- Infecting Bluetooth device with malicious software.

6) Man-in-the-Middle :- Interpreting and altering Bluetooth communication.

Done
26/10/24