D.A.V PUBLIC SCHOOL
Sector-14, Gurugram

Issue 2: 17 December 2018

#CyberSafetyAwareness

#MobileSafety

"Mobile phones are ubiquitous and indispensable, yet they have also given rise to a curious bundle of safety, security and privacy fears"

- Ankit Fadia

Mobile Usage:

Imagine a day without your mobile and you feel "Without my cell phone, I wouldn't

1. Make a call
2. Know the updates on my WhatsApp groups
3. Be able to use my e-wallet
4. Know what time it is
5. Be able to calculate
6. Take a snapshot at a picture-perfect time
7. Be able to wake up from an alarm in the morning
8. Find way in the dark"

And the list goes on….

A mobile is an all in one device. You name anything and you have it in your mobile- Aadhar card, PayTm, email, social networks, OLA etc. It has rather become a necessity than luxury.

But, while using mobiles **Balance** and **Discipline** is the key.

Use mobiles with caution not only for good health and safe financial transactions, but raising better human beings. Before allowing mobile usage to children help them understand basic netiquettes.

Be a role model -

- **Set a limit to the time spent online.**
- **Make way for family time.**
- **Follow basic netiquettes.**

Preventions for mobile theft:

1. **Record IMEI number:** Record the unique 15 digit IMEI number. This IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.
2. **Enable Device locking**: Use AutoLock to automatically lock the phone or keypad lock protected by passcode/security patterns to restrict access to your mobile phone.
3. **Use a PIN to lock SIM card and SD card:** Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN or on your SD card.

⇒ ***Note:*** *This is usually printed on the phone below the battery, or can be accessed by keying *#06# on most of the phones.*

Measures after losing your device

Use a mobile tracking feature in case your device gets lost:

Google Find My Device: Android Devices

Apple Find My iPhone: iOS Devices

Note : *This feature will not work in case your device is disconnected from internet or is switched off.*

Vulnerabilities & Solutions

Battery Drains off, System hangs up

Solution: **KEEP A CLEAN MACHINE**

Update the operating system: Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.

Delete when done: Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterwards, or we may have previously downloaded apps that are no longer useful or interesting to us. It's a good security practice to delete all apps you no longer use.

Unauthorized information access

Some apps can use the smartphone (without our knowledge)

1. to make phone calls
2. record conversations between the user and others
3. to access personal photos, music, videos, contacts, calendars, notes, financial information, location, email, identity, text messages etc. This stolen information could be used for identity theft or financial fraud.

Ways of unauthorised access to your device and their solutions:

1. **Public Wi-Fi network**

   Solution: Limit what you do on public WiFi and avoid logging in to key accounts like email and financial services on these networks. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection on the go. Connect only to a trusted network.

2. **Bluetooth in discoverable mode**

   Solution:

- Turn off applications [camera, audio/video players] and disable connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections ON may pose security issues and also cause to drain out the battery.
- You should turn off Bluetooth or set it to "undiscoverable". The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.
- Your mobile phone's serial number can also be downloaded and used to clone the phone. Change the name of the device to a different name to avoid recognition of your Mobile phone model.

  Note: The default name will be the mobile model number for Bluetooth devices.
- Put a password while pairing with other devices. The devices with the same password can connect to your computer.

Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected.

3. **Installing free apps/Getting lured by free offers/ Giving permissions to apps**

There are no free lunches in the world
- Bill Gates.

BEWARE OF FREE APPS.
PEOPLE WANT YOUR DATA!

Vulnerabilities & Solutions

Solution:

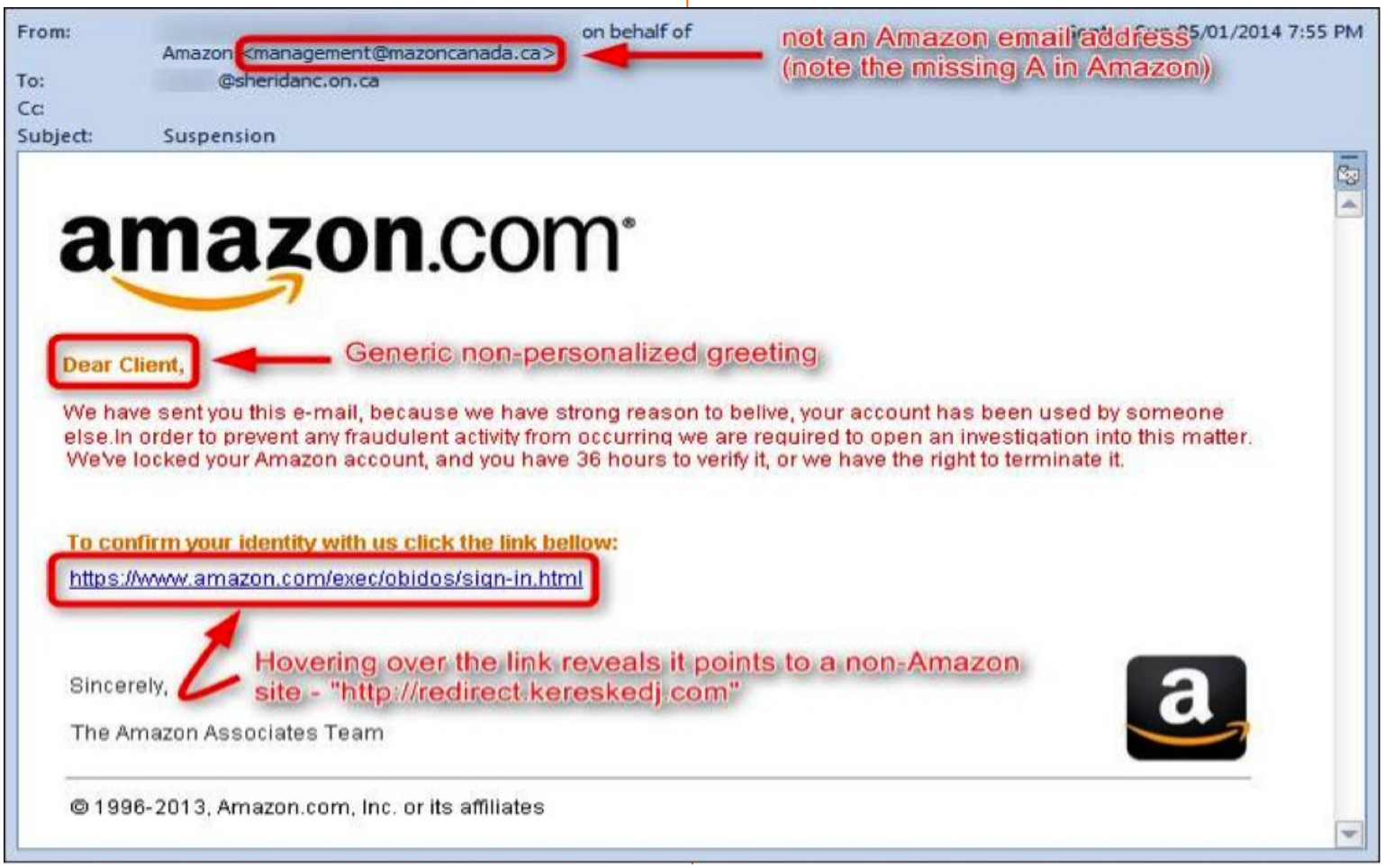
- Check authorization rights for each app in permissions/settings of your mobile.
- Always install applications from trusted sources. It is always helpful to check the features before downloading an application. Some applications may use your personal data.
- Do check the authenticity of an SMS or an E-mail containing an MMS message or a link to install software before actually installing it

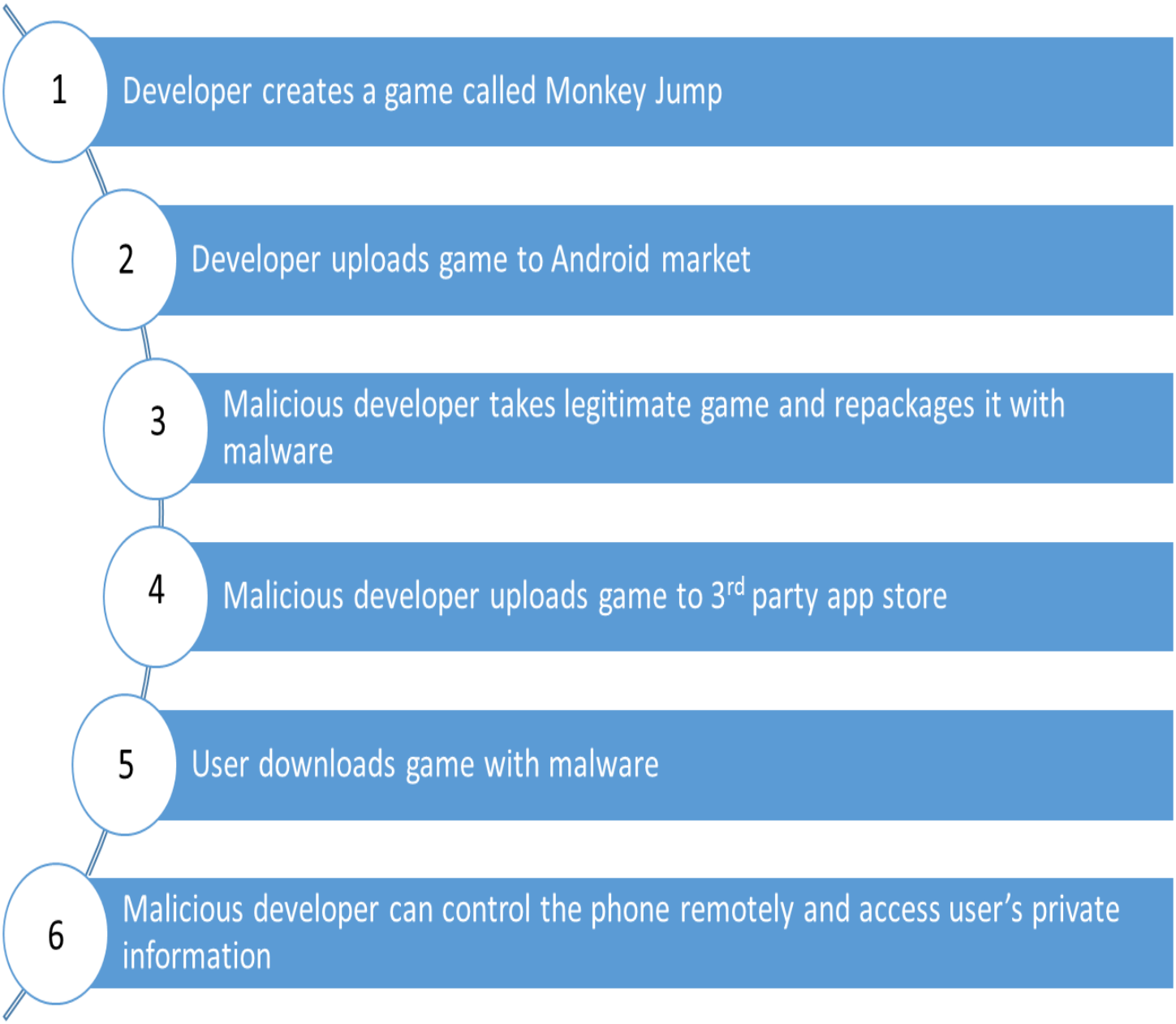
4. **Password cracking by guessing or following oil smudge pattern on the mobile or shoulder surfing**
   Solution:
   - Never leave your mobile device unattended.
   - Keep strong passwords/pattern/fingerprint

5. **Geo-tagging (attaching location information in the form of geographical metadata) in pictures.**
   Solution:
   Turn off Camera permissions to Location

6. **Phishing Scams (designed to trick you into providing information like passwords or account numbers. Often these messages and sites are very different to distinguish from those of your bank or other legitimate sources)**
   Solution: Never reveal any kind of personal information online.

7. **Vulnerable Applications are apps that contain flaws which can be exploited for malicious purposes. This can allow an attacker to access sensitive information, stop a service from functioning correctly, or download apps to your device without your knowledge.**
   Solution: Always install applications from trusted sources.





Data Security:

Backup data regularly: Backup data regularly and set up your phone such that it backs up your data when you sync it.

Reset to factory settings: Make sure to reset to factory settings when a phone is permanently given to another user to ensure that personal data in the phone is wiped out.

- When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated anti-virus.
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.

Reference :www.infosecawareness.in