openHPI Course: Cyberthreats by Malware

Protective Measures

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Protective Measures against Malware: **Program Updates** (1/2)

Program updates close system vulnerabilities and eliminate security risks

- Use of older software versions = security risk
- Risk of abuse of publicly known vulnerabilities

Install updates as soon as they are available

- Manufacturers do not find all errors during test phase
- Many security gaps in programs are often only discovered during the usage
  - □ Also through attacks or analysis by external experts
- Known security vulnerabilities can usually be closed by smaller update packages

Protective Measures against Malware: **Program Updates** (2/2)

Program updates

- Currently, most programs automatically provide information on available updates
- There are helper-applications that automatically check for updates of installed software
- Even good antivirus programs check that the installed software is up-to-date

But with all updates:

- Trustworthiness of source of updates must always be checked to ensure that the updates are genuine
- Otherwise, updates can become a vulnerability that could be exploited to malware installation or cyber attacks

Protective Measures against Malware: **Anti-Virus Software**

- **Anti-virus software** provides methods for detecting malware installed in the computer system
- Detects viruses, worms, trojans, spyware, scareware and other malware types
  - also called **anti-malware software**
- It also monitors Internet connections and warns about accessing unsafe websites
- The program should be a mandatory component of each system to ensure that the computer system is secure

➢ **Excursus on Anti-Virus Software**

Protective Measures against Malware: **Backups**

Many malware attacks on the Internet result in **data loss** or **damage**

- In case of data loss due malware or damage to the operating system, data can be restored using previously created **backup** copies
- Important and personal data must be **backed up regularly**
- Many systems offer automatic data backup at predefined intervals
- Store (encrypted) backup on external media or in the cloud
  - if an attacker manages to gain access to the computer, the user could lose access to backups

Protective Measures against Malware: **Firewalls**

- Firewalls monitor **Network Connections** and the corresponding traffic
- Can prevent unauthorized connection attempts
- Additional protection against network attacks, such as attacks from backdoors and botnets
- **Local firewall** only works on the machine on which it is installed
- **Network firewall** checks all network traffic and is usually installed on connection nodes between the local network and the Internet

➢ **Excursus on Firewalls**

Protective Measures against Malware: **“Healthy“ Suspicion – Always Be Careful!**

Suspicion is the most effective protection that could be done by the users against malware infections

- Best protection mechanisms are no longer effective if the user opens non-trustworthy content
- When installing new software, always **check manufacturer and origin** of the software
- **Verify signature** of the software to be installed / updates (can be done automatically)
- If a warning appears, a manual verification is necessary
- **Only install software that is really needed**
    - do not install unnecessary applications, additional features, or optional plugins - they provide an unnecessary access point for attackers

Protective Measures against Malware: **“Healthy“ Suspicion – Always Be Careful!**

- **Turn off active content** (Flash, Java, Active X) in the **web browser** by default as it provides a number of different attack and intrusion opportunities
- Open **email attachments** only if
  - □ the sender is known and the text can be assigned to the sender
  - □ an email with attachments was expected
- **Keep calm** with (often faked!) online warnings and requests for payment of fines
- Check installed software and **remove all unused** programs

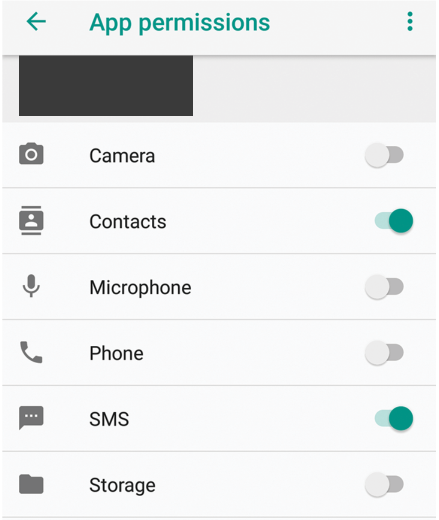
Protective Measures against Malware: **Mobile Devices (1/2)**

- Get applications **only from trusted sources**
  - preferably only from official App Stores
  - be careful with (new) apps with no or few ratings
- Keep apps and operating system of the mobile device always up to date
  - timely **installation of updates**
- **Create backups**
  - system can be restored from old backup in case of infection

Protective Measures against Malware: **Mobile Devices (2/2)**

Always grant apps only **minimal permissions**

- Could be set up during initial startup or in the settings
- Select permissions **according to the app's functions**
  - □ **Example**: Flashlight app does not require access to the contact list

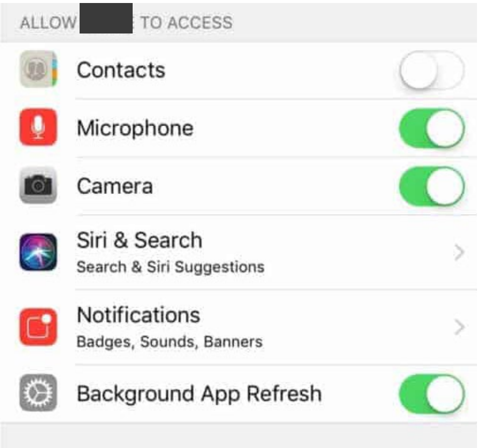


App permissions

[redacted]

Camera ○
Contacts ●
Microphone ○
Phone ○
SMS ●
Storage ○

Application permisions for Android



ALLOW [redacted] TO ACCESS

Contacts ○
Microphone ●
Camera ●
Siri & Search
Search & Siri Suggestions ›
Notifications
Badges, Sounds, Banners ›
Background App Refresh ●

Application permisions for iOS