Lezione 21 del 20-04-2023

Le truffe

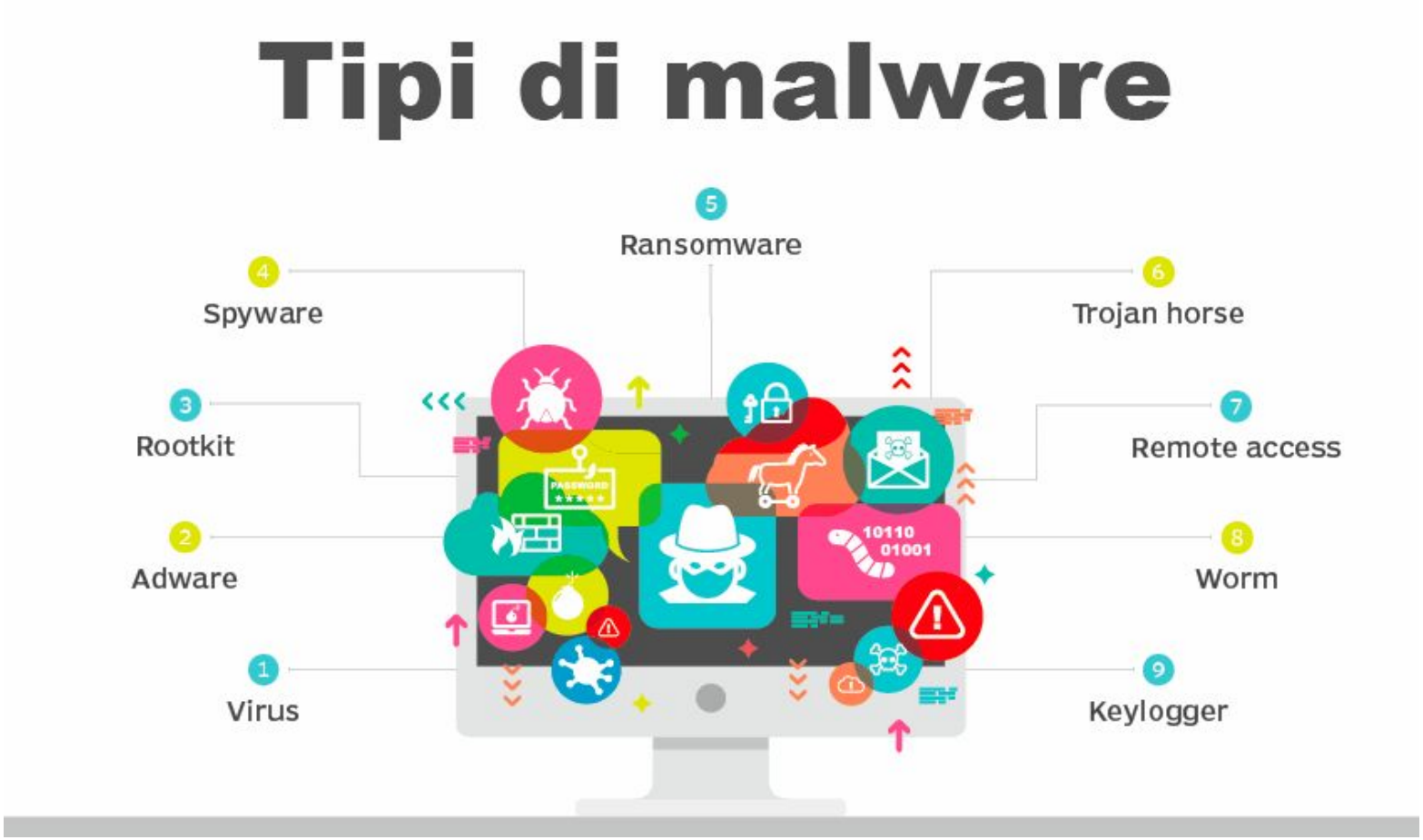
Corso android per smartphone

Docenti Dott.ssa Roberta Lai Ing. Massimo Terrosu

cadadie.it

Sicurezza e **Privacy** (S/P) TRUFFE

- **Il 96% dei mal(icius soft)ware colpisce Android, oggi abbiamo una nuova app dannosa ogni 10 secondi**



Sicurezza e **Privacy**

Spyware

Oggi gli smartphone contengono tante informazioni quindi può essere più utile spiare il dispositivo piuttosto che rubarlo

Troian "cavallo di Troia" o "captatori informatici" (usati per intercettazioni di Stato)

Es. Pegasus, lo spyware della società israeliana NSO usato per spiare giornalisti, attivisti e capi di Stato. L'attacco viene avviato tramite una videochiamata (prevalentemente su WhatsApp) in cui non serve che la vittima risponda.

Keylogger (controllare figli,consorti, dipendenti...)

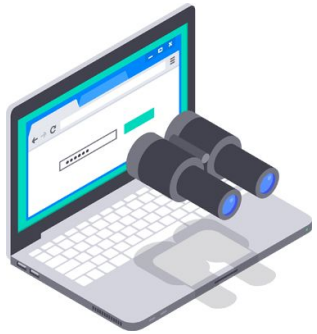
Uso malevolo dei sensori (WIFI,connettività, bluetooth, GPS, fotocamera, microfono, SIM….)

RISCHI delle reti Wi-Fi

Le reti pubbliche hanno sicurezze estremamente deboli.
Basta un semplice apparecchio dotato di due schede di rete Wi-Fi per creare un fake access point.
Evitare di collegarsi a reti Wi-Fi aperte, piuttosto utilizzare la rete 4G.

RISCHI del Bluetooth

BrakTooth può bloccare i dispositivi Bluetooth e conseguentemente indurre l'utente a connettersi ad uno specifico hardware Bluetooth malevolo.
E' importante fare l' update per i propri dispositivi Bluetooth.



RISCHI della fotocamera/microfono e GPS

Spie ambientali
Facebook sfrutta i sensori per profilare gli utente e creare gruppi omogenei.
I dati del GPS sono anche nelle fotografie.

RISCHI NFS

Mezzi di pagamento e carte di credito contactless.
Oggi alcune banche hanno sollevato a 50 euro il limite del prelievo senza PIN.
Esistono custodie che bloccano il trasferimento dei dati

Truffe

Le 3 tipologie più comuni di attacco Phishing

Il Phishing è una truffa attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornirgli informazioni personali

1 Phishing

Phishing via e-mail

2 Smishing

Phishing via SMS

3 Vishing

Phishing via telefono

COSA LE CARATTERIZZA

- ✓ Richiesta di un'azione da compiere con urgenza
- ✓ Richiesta di informazioni sensibili
- ✓ Presenza di link o allegati da scaricare

- ✓ Offerta imperdibile o intervento di sblocco
- ✓ Urgenza per non perdere l'occasione o per intervenire
- ✓ Presenza di un link che indirizza a un sito malevolo

- ✓ Chiamata dalla banca o organizzazione conosciuta
- ✓ Senso di urgenza legato a un possibile rischio
- ✓ Richiesta di informazioni sensibili, pin, numeri carte