

LEZIONE 16 DEL 10/03/2022

SICUREZZA  
PRIVACY



# CORSO ANDROID PER SMARTPHONE

Docenti Dott.ssa Roberta Lai, Ing. Massimo Terrosu

*cadadie.it*

# Sicurezza e Privacy



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

## Tipi di malware



# 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 utenti 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



# Sicurezza e Privacy

## Prevenzione contro gli SPYWARE

### - Autenticazione a due fattori (2FA)

Concetto di fattore:

qualcosa che conosciamo ( Password e/o domande di sicurezza)

qualcosa che abbiamo ( token OTP... )

qualcosa che possediamo ( impronta digitale, viso)

dove siamo (localizzazione smartphone)

### - Scaricare e installare applicazioni solo da app store ufficiali come Google Play

Scaricare con attenzione qualunque tipo di app.

Verificare:

il numero di download

le recensioni ( <https://it.trustpilot.com/>)

i permessi richiesti (non dare permessi non congrui con la tipologia di app)

il nome dell'autore.

### - Non eseguire mai il “root” dei dispositivi

### - Installare tempestivamente gli aggiornamenti del sistema e delle applicazioni

### - Effettuare il log out dalle applicazioni, specialmente bancarie

### - Cambiare spesso la password dell'account Google e delle Banche





## 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



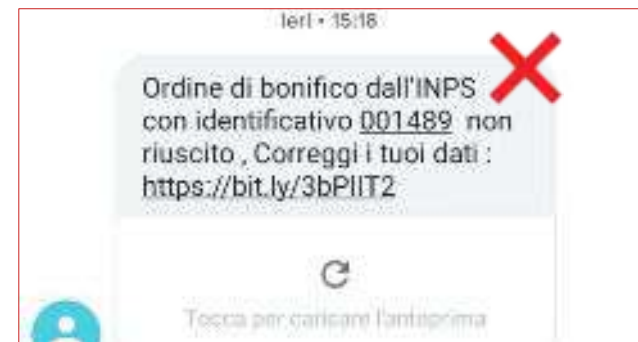
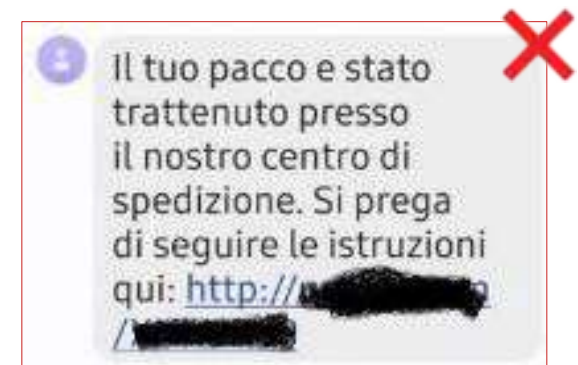
# Sicurezza e Privacy

## Truffe: mezzi di diffusione più utilizzati



### Messaggistica

### Truffe via SMS



# Sicurezza e Privacy



Come fare screenshot su tutti gli smartphone

Come fare gli screenshot sugli smartphone Samsung



1) Funzione integrata **Regist.schermo**



2) App **Mobizen Screen Recorder**



3) **ok Google**

*Impostazioni* > digitare nel motore di ricerca:  
*voice match*

Se non salva l'immagine mettere un flag su:  
*usa contesto dello schermo*

# Sicurezza e Privacy

## Truffe: mezzi di diffusione più utilizzati



### Messaggistica

Buono Spesa Carrefour  
Ricevi un buono di Carrefour del valore di € 100  
www.carrefour.com

Guarda: <http://mypromo.co/carrefour/>  
Un buono Spesa di 100€ Carrefour .  
Stanno celebrando il loro 60esimo anniversario e sono in quantità limitata. lo già l'ho preso. ❤️❤️

13:05 ✓

### Truffe via WhatsApp



Per esempio:

**Ikea** (concorso con buono da 500 euro ),  
**Zara** (Coupon da 150 euro),  
**H&M** (buono sconto da 100 euro),  
**Apple** (iPhone 7 a prezzi stracciati),  
**Carrefour** (buono spesa da 100 euro).

Se si clicca sul link, si accederà ad una pagina con un questionario da compilare per avere diritto allo “sconto”, che ruberà i dati personali.

In altri casi verrà richiesto di inoltrare il messaggio ad almeno 10 contatti per sbloccare la promozione. Oppure potrebbe attivare servizi in abbonamento che prelevano fino a 5 euro settimanali dal credito telefonico.

13:20

13:40

Oggi

Ho bisogno di un favore

09:57

Dimmi

10:36 ✓

Ho comprato da internet ma la mia carta di credito è scaduta posso usare la tua e ti faccio un bonifico

10:39

Truffa del bonifico (furto di identità)

Buono 150€ Zara  
Ricevi un coupon di Zara del valore di € 150  
www.zara.com

Appena presooo 😊

<http://ft3.co/zara/>

09:12



# Sicurezza e Privacy

## Truffe: mezzi di diffusione più utilizzati



### Social



Nei **Social** la tendenza è abbassare le difese per cui bisogna prestare maggiore attenzione a:

- >inviti da presunti amici
- >offerte vantaggiose inviate
- >comunicazioni da banca, poste, provider telefonici...
- >comunicazioni in situazioni di emergenza molto diffuse mediaticamente.

Un **altro tipo di attacco** più subdolo: è l' "URL Padding" .



Un messaggio contenente un link "camuffato" così:

*http://m.facebook.com-----validate---  
step1.rickytaylk.com/sign\_in.html*

sul display di uno smartphone sembrerà il link a Facebook, se cliccato indirizzerà verso un sito "fake" del tutto simile a Facebook, dove verrà chiesto di inserire le proprie credenziali Facebook.

# Sicurezza e Privacy



## Truffe: mezzi di diffusione più utilizzati

### Messaggistica

### Truffe in periodo di Covid



Gli Sms che il Ministero sta inviando ai vaccinati si prestano a essere veicolo di phishing.



Il messaggio falso che circola su WhatsApp

# Sicurezza e Privacy

---



## Truffe: altri mezzi di diffusione

**Truffe via Browser** (pericolosi su smartphone perchè hanno schermi piccoli)  
Banner malevoli (attivazione di un servizio in abbonamento) o richieste di consensi.

**Truffa del Robocall** rispondendo al telefono, si viene accolti da un messaggio registrato. L'obiettivo è quello di far rispondere con un "sì" a domande per autorizzare addebiti .

**Truffa dello squillo** riagganci dopo un solo squillo e di solito più volte al giorno .L' obiettivo è quello che l'utente richiami così da addebitargli gli alti costi di una telefonata all'estero.

**Truffa del QR code** (Quick Response) può contenere stringhe alfanumeriche  
**QR per pagamenti online** tramite app bancarie (poche verifiche)  
**QR come URL** (contengono link a siti web di phishing o un watering hole attack)  
**QR come numero di telefono fake**



Usare app tipo **QR Code Reader and Scanner di Kaspersky Lab Switzerland**



# Sicurezza e Privacy



## Truffa dello SIM swappig



Il truffatore ottiene i dati personali dell'utente tramite phishing



Il truffatore chiama l'operatore telefonico e, con tecniche di persuasione, ottiene il trasferimento del numero (SIM)



L'operatore telefonico trasferisce il numero dell'utente sulla SIM del truffatore



Il truffatore adesso riceve gli SMS e le chiamate della vittima che è ignara fino all'uso del telefono



Il truffatore bypassa facilmente la 2FA



Il truffatore ruba i soldi e cancella tutto

# Sicurezza e Privacy



## Truffa dello SIM swappig

La **SIM** crea una corrispondenza univoca tra la nostra “identità fisica” (la SIM) e la nostra “identità digitale” (il numero di telefono). La terminologia “**SIM swapping**” si riferisce all’atto di **trasferire da una SIM card a un’altra questa corrispondenza** con il nostro numero di telefono. Tale trasferimento può essere effettuato solo tramite operatore telefonico (con imbroglio, corruzione, documenti o dichiarazioni false etc...)

Prima del Sim Swapping è necessario catturare tutte le informazioni sensibili relative al cliente, al fine di ricevere **sul loro telefono il codice di autenticazione dell’operazione di bonifico**. Queste possono essere reperite con falsi sms, false telefonate, ricerche sui social e quantaltro precedentemente descritto

### I sintomi che dovrebbero metterci in allarme e cosa fare:

il cellulare, improvvisamente, non è più in grado di connettersi,  
chiamare immediatamente il Customer Service del nostro gestore telefonico ed eventualmente **blocca lo scambio della SIM.**

- ✗ Chiamate da un presunto operatore telefonico che ti informa che ci sono problemi di linea  
Non farci caso
- ✗ Potresti ricevere molte chiamate fastidiose che ti spingono a spegnere il telefono per non essere disturbato.  
Non farlo
- ✗ potresti ricevere un SMS con la stessa informazione  
Non fare niente ma:
  - controlla i tuoi conti online
  - contatta il Servizio Clienti della tua banca e blocca l’operatività temporaneamente





# Sicurezza e Privacy

## Come difendersi da un attacco

- > Non utilizziamo il nostro numero di telefono per processi di autenticazione a due fattori che prevedano come modalità di ricezione del secondo fattore di autenticazione l'invio di un SMS.
- > Usare solo altri sistemi one time password (via app).
- > Se la banca lo consente meglio utilizzare una verifica via email su casella protetta.
- > Se la banca lo consente configuriamo l'accesso sicuro a due fattori tramite l'app della banca, che può usare l'impronta digitale del telefono o un PIN segreto per autorizzare tutti gli accessi e le transazioni, rendendo di fatto obsoleto l'invio via SMS.
- > Controlla sempre l'indirizzo del mittente ed eventuali errori di battitura.

Da: Intesa Sanpaolo Private Banking <corrispondenti@intesa.com> [sic] <corrispondenti@intesa.com>  
Data: 4 Maggio 2016 ore 11:06  
A: [il tuo indirizzo email]  
Oggetto: Aggiornamento del numero di cellulare (il tuo servizio)

**ATTENZIONE AL MITTENTE**  
*email non ufficiale*

**Intesa Sanpaolo PRIVATE BANKING**

Bonizio Clienti

Come anticipato in precedenza, tutti i clienti avranno presto bisogno di confermare il servizio tramite SMS o tramite servizio PUSH sull'applicazione mobile.

Per confermare il servizio il codice QR-KEY va inserito al telefono dal 4 maggio 2016.

Per accertarsi di poter confermare il servizio, controlla le impostazioni di autenticazione che il tuo numero di cellulare ha aggiornato. Assicurati che il numero di cellulare è corretto, il servizio push è funzionante e impostato correttamente.

**CLICCA QUI**

*non ti chiederemo mai di confermare via mail le tue credenziali*

Intesa Sanpaolo Private Banking opera con maggiore sicurezza e serenità per la sua clientela online. Contribuisce a mantenere i nostri clienti al sicuro tramite SMS e notifica push. Per favore assicurati che i dettagli siano corretti per poter confermare il servizio tramite SMS e tramite l'applicazione mobile dal 4 maggio 2016.

Intesa Sanpaolo Private Banking ti suggerisce di verificare che il tuo numero di telefono e i tuoi dati personali che richiedi per l'accesso di credenziali e di sicurezza siano corretti.

*errori di battitura*

# Sicurezza e Privacy

## Come difendersi da un attacco



il mittente è corretto  
MA... Attenzione!!!!

**SMS autentici**

Gruppo ISP >

Messaggio  
mar 29 apr, 17:32

O-Key SMS - Usa [453959](#)  
per entrare nel sito della tua banca online

mar 30 apr, 17:06

O-Key SMS - Usa [420657](#)  
per autorizzare

mar 30 apr, 17:10

Intesa Sanpaolo: Gentile Cliente ti invitiamo a metterti urgentemente in contatto con il nostro ufficio prevenzione frodi chiamando il numero verde: [800940828](#)

**SMS fraudolento (smishing)**

ora i frodatori possono utilizzare il nome corretto "Gruppo ISP" per mimetizzarsi tra gli SMS ufficiali

**ATTENZIONE AL LINK numero non ufficiale**

Verificare che il numero VERDE non sia un fake

# Sicurezza e Privacy



**Cosa fare qualora per sbaglio o intenzionalmente si sia cliccato sul link:**

1 formattare il dispositivo dal quale hai cliccato e ripristinare le impostazioni di fabbrica

2 informare tutti i contatti in rubrica di cestinare i messaggi provenienti dalla propria utenza

3 modificare tutte le password utilizzate nel dispositivo relative al sito poste italiane o della propria home banking

4 se però hai fornito i tuoi dati bancari devi assolutamente bloccare le carte e sporgere denuncia presso la polizia postale

# Sicurezza e Privacy



## SEGNALI CHE IL TUO SMARTPHONE HA UN VIRUS

**Consumo anomalo del traffico dati**

Un virus potrebbe generare un elevato traffico dati. Oltre alle info fornite dal sistema operativo è possibile fare analisi su questa attività da app specifiche | [click qui](#) |

**Addebiti fraudolenti**

Le app malware potrebbero effettuare acquisti in-app o tentativi del recupero premium non desiderati. Scopri come verificarli | [click qui](#) |



**App che si chiudono da sole con regolarità**

A causa di un virus le nostre APP potrebbero avere dei malfunzionamenti e chiudersi spesso da sole. Scopri come verificare il problema | [click qui](#) |

**Improvvisi aperture di Popup**

Uno dei problemi più fastidiosi, indicatori della presenza di malware nel telefono da rimuovere. Scopri come verificare il problema e se possibile rimuoverlo | [click qui](#) |



**Durata molto limitata della batteria**

Uno dei segnali più forti è proprio una improvvisa riduzione della durata della batteria. Scopri come verificare il problema | [click qui](#) |

**La presenza di APP fake o sconosciute**

Scopri come controllare lo stato di certificazione delle APP e visualizzare l'elenco delle app che possiedono i privilegi di amministratore | [click qui](#) |



**Un elevato surriscaldamento del telefono**

Il virus potrebbe provocare il lavoro in notte CPU del telefono e lo RAM e generare il problema del calore eccessivo. Scopri come verificare il problema | [click qui](#) |

**Rallentamenti dello smartphone**

Improvvisamente il telefono è lento? Se vedi questo simbolo per escludere che si tratti di un problema di memoria piena potresti verificare con un | [click qui](#) |



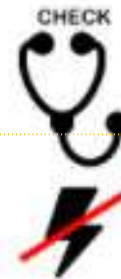
**Email di spam nella posta inviata**

Fate attenzione alle email che vengono inviate nella vostra posta. Un controllo ogni tanto è davvero importante. Andate nella posta inviata e verificate la presenza di email che non vi appartengono



# Sicurezza e Privacy

## Android security checkup 10 passi per uno smartphone più sicuro



Google ha inserito sistemi di protezione avanzati all'interno di Android. Quel che segue è un check up che dovrebbe essere fatto una volta all'anno.

**Step 1:** Verificare le app non più utilizzate e disinstallarle.

**Step 2:** Verificate i permessi forniti alle app e disinstallare quelle con permessi NON congrui.

Inoltre per verificare le app che hanno accesso all'account google (drive, google foto...)  
"https://myaccount.google.com/permissions"

**Step 3:** Verificare che Google Play Protect sia attivato.

**Step 4:** Verificate le password salvate nel vostro account e usate password robuste.

**Step 5:** Verificate l'utilizzo dell'autenticazione a due fattori (2FA).

Come attivare la 2FA

Vai alla pagina dell'ACCOUNT(gestisci account)

Vai sulla scheda SICUREZZA e attiva il 2FA

<https://myaccount.google.com>



# Sicurezza e Privacy

---



**Step 6:** Ottimizzare la sicurezza del proprio Lock Screen  
Il lock screen è la porta di ingresso al vostro smartphone.

**Step 7:** Pulisci l'elenco dei tuoi device connessi  
Ogni qualvolta collegate un nuovo device ad un account questo viene aggiunto  
<https://myaccount.google.com/security>

**Step 8:** Verificate che l'app Find My Device sia attiva e inserite nei preferiti la versione web  
<https://www.google.com/android/find?u=1>

**Step 9:** Verificate l'account Google  
Google conosce moltissime cose su di voi per eliminare il contenuto dell'account.  
<https://myaccount.google.com/inactive?pli=1>

**Step 10:** Anche l'account Google necessita di un ckeckup  
<https://myaccount.google.com/>  
Ed anche  
<https://myactivity.google.com/myactivity>

Per proteggere l'account Google, un'altra via è l'utilizzo di autenticatori hardware come **Google Titan Security Keys** o **YubiKey**, che in realtà superano il concetto di 2FA e abbracciano il nuovo standard U2F (Universal 2nd Factor) di FIDO Alliance, che innalza ulteriormente il livello di sicurezza del sistema di autenticazione.