IL MALWARE CHE COLPISCE
IL MOBILE BANKING

IL MALWARE PUÒ COSTARVI CARO

Il malware che colpisce il mobile banking è appositamente studiato per rubare i dati finanziari eventualmente memorizzati su un dispositivo.

COME SI DIFFONDE?

- **Visitando siti dannosi**
- **Scaricando app dannose**
- **Tramite phishing**

QUALI SONO I RISCHI?

- **Furto dei dati di autenticazione personale**
- **Prelievi non autorizzati**

COSA POTETE FARE PER PROTEGGERVI?

- Scaricate l'app mobile ufficiale della vostra banca e assicuratevi ogni volta di visitare il sito autentico della vostra banca. (https://)
- Evitate di connettervi automaticamente al vostro sito o alla vostra app di banking online.
- Non condividete con né rivelate a nessuno il vostro numero di carta di credito o la vostra password.
- Se possibile, installate un'app di mobile security in grado di segnalare eventuali attività sospette.
- Se perdete il vostro telefono cellulare o cambiate il vostro numero, contattate la vostra banca per fare aggiornare i vostri dati personali.
- Non condividete alcun dato relativo al vostro account tramite messaggi di testo o e-mail.
- Utilizzate sempre una rete Wi-Fi protetta per connettervi al sito mobile o all'app della vostra banca. Non fatelo mai utilizzando una rete Wi-Fi pubblica!
- Controllate frequentemente i vostri estratti conto.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

EDUCatt Ente per il Diritto allo Studio Universitario dell'Università Cattolica

UNIVERSITÀ CATTOLICA del Sacro Cuore

RANSOMWARE
MOBILE

DITE ADDIO AI VOSTRI FILE PERSONALI

Il ransomware è un tipo di malware in grado di tenere in ostaggio un dispositivo mobile ed i dati in esso contenuti fino al pagamento di un riscatto. Questo tipo di malware blocca lo schermo del dispositivo o impedisce di accedere ad alcuni dei file e delle sue funzioni.

COME SI DIFFONDE?

Visitando siti compromessi.

Scaricando versioni falsificate di app normali.

Facendo clic su link malevoli e allegati alle e-mail di phishing.

QUALI SONO I RISCHI?

Potrebbe rendersi necessario il ripristino ai valori di fabbrica del dispositivo con conseguente perdita di tutti i dati.

Un utente malintenzionato può avere accesso completo al vostro dispositivo e condividere i vostri dati con soggetti terzi.

COSA POTETE FARE PER PROTEGGERVI?

Effettuate un backup frequente dei vostri dati e aggiornate regolarmente tutte le vostre app e il sistema operativo.

Evitate di acquistare app presso app store di terze parti.

Se possibile, installate un'app di mobile security in grado di segnalare se il dispositivo è stato compromesso.

Diffidate di e-mail e siti sospetti o che sembrano troppo belli per essere veri.

Non concedete a nessuno i diritti di amministratore del dispositivo.

Non pagate alcun riscatto. Se lo fate, finanzierete dei criminali incoraggiandoli a continuare le loro attività illegali.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

EDUCatt Ente per il Diritto allo Studio Universitario dell'Università Cattolica

UNIVERSITÀ CATTOLICA del Sacro Cuore

MINACCE VIA INTERNET

VALUTATE BENE PRIMA DI FARE CLIC

Se il vostro dispositivo smette di funzionare, potreste perdere il vostro denaro e i vostri dati personali oltre ai dati memorizzati. Non fatevi raggirare!

COME PUÒ SUCCEDERE?

ATTACCHI DI PHISHING: gli utenti vengono ingannati e convinti a fornire i propri dati presentandosi come un'entità affidabile. Si diffondono tramite e-mail, messaggi di testo o piattaforme di social network.

ESPLORAZIONE DI SITI: il vostro dispositivo mobile potrebbe infettarsi semplicemente visitando un sito non sicuro.

DOWNLOAD DI FILE: un'e-mail può contenere link e allegati dannosi.

PERCHÉ È EFFICACE?

I dispositivi mobili sono COSTANTEMENTE CONNESSI a Internet.

Le DIMENSIONI RIDOTTE DELLO SCHERMO DI UN DISPOSITIVO MOBILE rappresentano un limite generale. I browser dei dispositivi mobili visualizzano gli URL su uno schermo dallo spazio limitato, pertanto è difficile vedere se un determinato dominio è autentico.

L'UTENTE NUTRE UNA FIDUCIA IMPLICITA nella natura personale di un dispositivo mobile.

COSA POTETE FARE PER PROTEGGERVI?

Siate sospettosi se ricevete un SMS o una telefonata da un'azienda che vi chiede di fornire i vostri dati personali. Potete verificare l'autenticità della chiamata o del messaggio ricevuto richiamando direttamente l'azienda al loro numero.

https://

Quando navigate su Internet con il vostro dispositivo mobile, assicuratevi che la connessione sia protetta tramite HTTPS. Potete sempre controllare la parte iniziale dell'URL.

Non fate mai clic su un link o un allegato contenuto in un'e-mail o un SMS indesiderato. Eliminatelo immediatamente.

^BE:%}
W@RY
*)Z#$=

Diffidate dei siti dalla grammatica povera, con errori ortografici o a bassa risoluzione.

Se possibile, installate un'app di mobile security in grado di segnalare eventuali attività sospette.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

EDUCatt Ente per il Diritto allo Studio Universitario dell'Università Cattolica

UNIVERSITÀ CATTOLICA del Sacro Cuore

APPS

SOLO UN GIOCO?

Installate solo applicazioni provenienti da app store ufficiali

DATE UN'OCCHIATA ALLE RECENSIONI DI ALTRI UTENTI

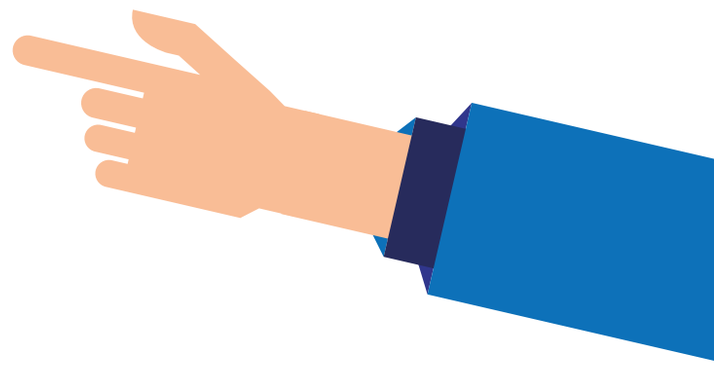
Prima di scaricare un'app, fate una ricerca sia sull'app che sugli autori.
Siate cauti con i link che ricevete per e-mail e fate attenzione ai messaggi di testo che potrebbero indurvi a installare app di terze parti o fonti sconosciute.

VERIFICATE LE AUTORIZZAZIONI DI UN'APP

Controllate a quali tipologie di dati può accedere l'app e se può condividere i vostri dati con parti esterne.
Un'app ha proprio bisogno di tutte quelle autorizzazioni?
Nel dubbio, non scaricate.

INSTALLATE UN'APP PER LA SICUREZZA MOBILE

Questa esaminerà tutte le app presenti sul vostro dispositivo e ogni app nuova che installerete successivamente avvisandovi nel caso in cui dovesse essere rilevato un software dannoso.



EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

EDUCatt Ente per il Diritto allo Studio Universitario dell'Università Cattolica

UNIVERSITÀ CATTOLICA del Sacro Cuore