Non cliccare su quel Link!!

«Evitare di cadere nelle trappole dei messaggi truffa e non mettere in pericolo i nostri soldi»

Sanremo 7 GENNAIO 2025

Rotary Club Sanremo Hanbury

LA MAGIA DEL ROTARY

IL COMPLICE DEL TRUFFATORE E'

LA VOSTRA VELOCITA' / FRETTA!

CADERE NELLA TRAPPOLA DEL MALFATTORE E' MOLTO FACILE:

PUO' CAPITARE A CHIUNQUE.

ED ECCO ADESSO ALCUNI ESEMPI DI TRAPPOLE

con relativi consigli

«EMAIL DI PHISHING BANCARIO»

Il Phishing si riferisce a email fraudolente che ingannano i destinatari nella condivisione delle proprie informazioni personali, finanziarie o di sicurezza

COME FUNZIONA?

Le email possono **SEMBRARE** identiche ai tipi di corrispondenza che le vere banche inviano:

Replicano i **LOGHI**

Chiedono si scaricare un documento o **FARE CLIC SU UN LINK**

Usano un linguaggio che trasmette senso di **URGENZA**

COSA PUOI FARE?

Tieni aggiornato l'ANTIVIRUS

Presta attenzione alla mail bancaria se TI RICHIEDE INFORMAZIONI SENSIBILI (password del cc online)

Controlla la **grammatica** e **ortografia** del testo

Non rispondere alla mail sospetta, ma inoltrala alla tua banca (NON FARE RISPONDI)

Non cliccare sul LINK e non SCARICARE l'allegato

IN CASO DI DUBBIO, CONTROLLA IL SITO WEB DELLA TUA BANCA O TELEFONA AL TUO GESTORE E FAI CONTROLLARE I MOVIMENTI DEL CONTO

«SMS DI PHISHING BANCARIO»

Lo SMISHING (dalla combinazione di SMS e Phishing) è il tentativo da parte dei truffatori di acquisire informazioni personali, finanziarie o di sicurezza tramite SMS

COME FUNZIONA?

L'SMS ti chiederà in genere di fare CLIC su un LINK o di chiamare un numero di telefono per «verificare», «aggiornare» o «riattivare» il tuo account.

Ma il Link porta ad un sito web FASULLO, che somiglia al 100% a quello autentico e il numero di telefono porta ad un truffatore che finge di essere la società legittima

COSA PUOI FARE?

NON CLICCARE SUL LINK che ricevi da SMS indesiderati

Non essere **FRETTOLOSO.** Prendi il tuo tempo e fai dei controlli appropriati prima di rispondere

NON RISPONDERE mai ad un SMS che richiede il tuo PIN o la PASSWORD del tuo conto o qualsiasi altra credenziale di sicurezza

SE PENSI CHE CI SIA LA POSSIBILITA' CHE TU ABBIA RISPOSTO AD UN TESTO DI SMISHING E FORNITO I TUOI DATI BANCARI, **CONTATTA IMMEDIATAMENTE LA TUA BANCA**

«TELEFONATE DI VISHING BANCARIO»

Il VISHING (dalla combinazione di Voice e Phishing) è una truffa telefonica

COME FUNZIONA?

Il truffatore cerca di indurre la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a TRASFERIRE loro del denaro.

COSA PUOI FARE?

Fai attenzione alle chiamate indesiderate.

Segnati il numero del chiamante e avvisalo che lo richiamerai.

Per verificare la loro identità, cerca il numero di telefono della TUA BANCA e contattali direttamente.

Non dare credito al truffatore chiamandolo sul numero che LUI ti fornisce (potrebbe trattarsi di un numero falso o contraffatto)

I truffatori possono trovare le tue informazioni di base attraverso i Social Media. NON PRESUMERE CHE CHI TI CHIAMA SIA AUTENTICO!

Non condividere il tuo PIN della carta di credito o Bancomat o password del conto online. LA TUA BANCA NON TE LI CHIEDERA' MAI.

NON TRASFERIRE DENARO SU ALTRO CONTO A RICHIESTA.

SE PENSI CHE SIA UNA FINTA CHIAMATA, SEGNALALO ALLA TUA BANCA

«TRUFFE SUGLI ACQUISTI ON LINE»

Gli acquisti online spesso sembrano proprio un buon affare, ma devi stare attento alle truffe

COME FUNZIONA?

Un'email, un pop up che contiene un'offerta speciale o un affare a tempo o un premio

Per non perdere l'offerta ti viene chiesto di fare SUBITO un bonifico

L'offerta ti richiede i dettagli del tuo conto o il pagamento

L'articolo è offerto a un prezzo MOLTO BASSO e spesso giustificato con l'indicazione «acquistato per errore» o altre scuse. I contatti avvengono solo via mail o telefono

Non hai ricevuto il prodotto né sei riuscito a contattare il venditore

COSA PUOI FARE E NON FARE?

Attenzione agli annunci di affari spropositati o prodotti miracolosi

Fai ricerche sul venditore e leggi le recensioni

Verifica che ci sia un numero di telefono, un indirizzo, un profilo social e soprattutto una POLITICA DI RESO E RIMBORSO.

Non pagare con un bonifico o trasferimento di denaro. Meglio la Carta di Credito e meglio ancora, utilizza la CARTA VIRTUALE

Se il prodotto non arriva, contatta il venditore. Se non ricevi nessuna risposta, contatta la tua banca.

Verifica che il sito internet del venditore abbia nell'indirizzo il simbolo del **LUCCHETTO** e che inizi con **HTTPS://**

«TRUFFE DI INVESTIMENTO»

Le comuni truffe di investimento possono includere opportunità di investimento redditizie quali: azioni, obbligazioni, criptovalute, metalli rari, investimenti immobiliari all'estero o energie alternative

COME FUNZIONA?

Ti vengono promessi rendimenti rapidi e ti viene assicurato che l'investimento è sicuro

L'offerta è disponibile solo per un tempo limitato

Ricevi ripetutamente una telefonata indesiderata

L'offerta è disponibile solo per te e ti viene chiesto di non condividerla

COSA PUOI FARE?

Assicurati sempre una consulenza finanziaria imparziale prima di consegnare denaro o fare un investimento

Rifiuta le vendite telefoniche relative ad opportunità d'investimento

Diffida delle offerte che promettono un investimento sicuro, rendimenti garantiti e grandi profitti

Attenzione alle truffe future. Se hai già investito in una truffa, è probabile che i truffatori ti prendano di mira nuovamente o vendano i tuoi dati ad altri criminali

Contatta la polizia se sospetti qualcosa

«TRUFFA SENTIMENTALE»

I truffatori prendono di mira le vittime sui siti di incontri online, ma possono utilizzare anche i social media o le mail per prendere contatto

QUALI SONO I SEGNALI?

Qualcuno che hai recentemente incontrato online dichiara di provare forti sentimenti per te, e ti chiede di chattare in privato

I loro messaggi sono spesso vaghi e scritti male

Il loro profilo online non è coerente con ciò che raccontano

Potrebbero chiederti di inviare foto o video personali

Prima ottengono la tua fiducia, poi ti chiedono denaro, regali

Se non invii il denaro, possono provare a ricattarti. Se lo invii ne chiederanno di più

COSA PUOI FARE?

Fai molta attenzione alle informazioni personali che condividi sui social

Sii cauto e fai delle domande

Fai ricerche sulla foto e sul profilo della persona per vedere se il materiale è stato usato altrove

Fai attenzione agli errori di ortografia

Non condividere materiale compromettente che possano usare per ricattarti

Se incontri di persona, informa parenti ed amici su dove stai andando

Non traferire denaro per conto di qualcun altro: il riciclaggio di denaro è un reato penale

«IL MULING»

Se qualcuno ti chiede di trasferire del denaro utilizzando il tuo conto corrente in cambio di un compenso, potresti diventare complice di un reato finanziario, senza neanche saperlo

COME RICONOSCERLO?

Il messaggio contiene un annuncio di lavoro che promette un'elevata remunerazione su siti di lavoro o social media o anche via mail o sms

Il messaggio contiene un'offerta vantaggiosa che prevede un compenso qualora tu accetti di ricevere temporaneamente dei soldi sul tuo conto oppure di prelevare contanti da consegnare a qualcuno o da versare su un conto estero

COSA FARE O NON FARE?

Non aprire mai un conto corrente su richiesta di qualcuno che hai appena conosciuto

Non permettere che il tuo conto venga utilizzato per conto di altri

Non fornire mai i tuoi dati bancari ad altri, a meno che siano persone che conosci e di cui ti fidi

Non lasciarti ingannare dalle offerte non richieste di soldi facili: se sembra troppo bello per essere vero, probabilmente non lo è!

Fai ricerche sull'azienda che offre il lavoro e affidati sempre a siti accreditati e consigliati

Se credi di essere coinvolto, interrompi immediatamente i trasferimenti di denaro, avvisa la tua banca e la Polizia di Stato.

Come difendersi dalle frodi online

Adotta i comportamenti giusti per proteggere al meglio le tue informazioni personali

Verifica spesso i movimenti del tuo conto e delle tue carte. Puoi farlo ogni volta che vuoi, online o dall'app

Non lasciare incustoditi i tuoi dispositivi portatili, tablet e cellulare

Conserva i tuoi codici personali con cura, tienili segreti e non comunicarli a nessuno. Evita di condividere sui social network anche informazioni private come la data di nascita, indirizzo, foto di casa o del posto dove lavori

Per accedere ai servizi online di qualunque sito usa sempre e solo link sicuri (meglio se salvati tra i tuoi preferiti)

Assicurati di scaricare e utilizzare App provenienti solo dagli store ufficiali

Aggiorna sempre l'app di mobile banking. Per aumentare la sicurezza del tuo smartphone, imposta un codice di blocco dello schermo

Rafforza le tue password e non memorizzarle sul browser. Ricordati di aggiornarle spesso (una volta al mese)

Non affidare mai la carta a terze persone, neanche a un familiare, per eseguire operazioni (nel caso, richiedi una carta aggregata intestata alla persona che ne ha bisogno)

Installa nel tuo computer un antivirus che includa una funzione antiphishing e tienilo sempre ben aggiornato

Annota sempre e porta con te i numeri di telefono di emergenza per il blocco della carta. Ricorda che puoi farlo anche online e da app

COOKIE 1/3

Cosa sono i **cookie?**

I cookie sono piccoli file di testo che conservano scelte, opzioni e selezioni degli utenti fatte sui siti internet

Tutte le volte che navighiamo su un sito, vengono salvati dati e informazioni

Ci sono cookie utili alla gestione della navigazione e altri che tracciano le nostre abitudini comportamentali come ad esempio per gli acquisti on line

Quante volte ci è capitato di visitare un sito per acquistare delle scarpe e ritrovarle pubblicizzate anche su altri portali?

COOKIE 2/3

I RISCHI dei cookie

I cookie possono essere utilizzati sia per scopi leciti, come nel caso dei costruttori dei siti, sia per scopi illeciti.

Possono essere manipolati o avvelenati (poisoning) dagli hacker. Sono utilizzati per carpire e memorizzare informazioni, violare la privacy dell'utente e rubargli l'identità digitale.

L'accesso ai cookie da parte dei criminali informatici può avvenire su PC infettati da un virus o nello scambio di informazioni sulla rete che il PC utilizza per dialogare con il sito.

COOKIE 3/3

COME POSSIAMO TUTELARCI?

1. Leggiamo attentamente il banner informativo che ogni sito, per obbligo di legge, deve esporre. Informiamoci sui vari tipi di cookie utilizzati! Prima di chiudere un banner dedichiamo qualche minuto alla sua lettura, soprattutto se nel sito dove siamo forniamo parecchie informazioni personali.

2. Gestiamo la cancellazione dei cookie. Con il tempo, i cookie crescono e si accumulano sul computer diventando una potenziale "miniera" di dati personali a disposizione anche di malintenzionati. Facciamo sempre pulizia!

3. Navighiamo in anonimo. I browser hanno funzioni che ci permettono di non salvare dati sul nostro PC. La navigazione anonima potrebbe risultare meno fluida e più complicata ma ci permette di ridurre i rischi derivanti da potenziali attacchi informatici.

MALWARE 1/5

Tra i più pericolosi e insidiosi, il malware può essere installato, a tua insaputa, sui dispositivi che usi per accedere al sito della tua banca, con lo scopo di trafugare dati riservati

Il Malware è un pezzo di software malevolo in grado di immettersi all'interno di un sistema senza autorizzazione,

con lo scopo di rubare o manomettere dati privati o aziendali, arrecare danno più o meno gravi al sistema informatico nel quale è in uso, o infine

spiare le vittime a scopo di estorsione

MALWARE 2/5

Tra i più pericolosi e insidiosi, il malware può essere installato, a tua insaputa, sui dispositivi che usi per accedere al sito della tua banca, con lo scopo di trafugare dati riservati

Come vengono diffusi?

- Email di phishing contenenti file allegati in formato apparentemente innocuo o link diretti a siti web poco affidabili
- Download di programmi o giochi in versione demo
- Pubblicità apparentemente normali diretti a URL poco affidabili
- Dispositivi USB infetti, utilizzati soprattutto in ambienti aziendali per danneggiare i dispositivi
- Intrusione diretta nelle reti aziendali o locali tramite la violazione dei parametri di sicurezza informatica
- App apparentemente innocue scaricabili da App Store non ufficiali.

MALWARE 3/5

Tra i più pericolosi e insidiosi, il malware può essere installato, a tua insaputa, sui dispositivi che usi per accedere al sito della tua banca, con lo scopo di trafugare dati riservati

Cosa fare e non fare

- Ti suggeriamo di tenere sempre aggiornati il sistema operativo, i programmi antivirus e altri software o app presenti sui tuoi dispositivi
- Non installare mai app di dubbia provenienza o disponibili su store non ufficiali
- Non cliccare sui link contenuti in mail inaspettate o sospette o all'interno di SMS
- Cerca e scarica solo versioni ufficiali dei software da siti sicuri
- Quando navighi in internet non cliccare su link sospetti, pop-up o finestre di dialogo
- Non utilizzare account con privilegi amministrativi per le ordinarie attività quotidiane

MALWARE 4/5

Tra i più pericolosi e insidiosi, il malware può essere installato, a tua insaputa, sui dispositivi che usi per accedere al sito della tua banca, con lo scopo di trafugare dati riservati

Quali sono i segnali?

- Il tuo dispositivo elettronico potrebbe darti dei segnali utili:
- Le prestazioni del dispositivo iniziano a diminuire (es. pc lento, batteria si scarica più velocemente)
- L'utilizzo delle risorse di sistema è particolarmente elevato
- Durante la navigazione in rete compaiono numerosi pop-up advertising non richiesti e non autorizzati
- L'antivirus smette di funzionare correttamente e non risponde
- Nel browser di ricerca sono comparse barre di strumenti indesiderate, che non sono modificabili e risulta impossibile tornare alle impostazioni predefinite del motore di ricerca

MALWARE 5/5

Tra i più pericolosi e insidiosi, il malware può essere installato, a tua insaputa, sui dispositivi che usi per accedere al sito della tua banca, con lo scopo di trafugare dati riservati

Sei stato infettato?

- Segnala l'evento alla Polizia di Stato
- Scollega i tuoi device da internet o altre connessioni di rete (ad es. la rete wi-fi di casa) il più presto possibile al fine di prevenire che l'infezione si propaghi
- Formatta il disco rigido del device infetto
- Reinstalla il sistema operativo e le app
- Fai partire ogni aggiornamento disponibile
- Recupera i tuoi file bloccati dal tuo device di back-up (se ne hai uno)

STRUMENTI DI DIFESA

1. Leggi attentamente i messaggi e le email che ti arrivano. Verifica che il mittente sia vero
2. Utilizza delle PASSWORD forti (non date di nascita, informazioni conosciute ad altri, serie di numeri o lettere tipo 12345, qwerty, ecc.)
3. Installa e manutieni l'antivirus (anche sullo smartphone!)
4. Utilizza un sistema di blocco schermo per il cellulare
5. **Ricorda che NESSUNO TI REGALERA' MAI NULLA!! Non abboccare e non fare mosse AFFRETTATE!!!**