Social Network

Utilizzare le impostazioni di privacy a disposizione per impedire la visualizzazione delle proprie informazioni a persone non autorizzate.

Prestare sempre estrema attenzione ai link su cui si clicca (gli hacker possono compromettere l'account di un amico e adoperarlo per diffondere malware o altri contenuti malevoli).

Non accettare richieste di amicizia da persone che non si conoscono, possono nascondere account falsi creati appositamente per carpire le vostre informazioni.

Nascondere il proprio indirizzo e-mail (gli intrusi potrebbero rubare il vostro account grazie all'indirizzo e-mail pubblicato).

Reti Aperte

Evitare di usare l'internet banking o altre attività che richiedano dati personali su reti wireless pubbliche (aeroporti, bar, hotel e altri luoghi pubblici) perché le comunicazioni potrebbero essere intercettate.

Aggiornarsi

Tenersi sempre informarti sulle nuove minacce informatiche. Conoscere vuol dire iniziare a difendersi.

BANCO DELLE TRE VENEZIE SPA

EM-RISK

BANCO DELLE TRE VENEZIE SPA

Sicurezza Informatica: Consigli Pratici

La Sicurezza Informatica sta diventando un tema sempre più sensibile nella società moderna per via della crescente informatizzazione dei servizi e del conseguente aumento del numero degli attacchi.

Il Banco delle Tre Venezie è consapevole che è necessario un approccio integrato per la soluzione di questo problema pertanto, oltre a dotarsi di sistemi e standard di sicurezza elevati per i servizi offerti, ha voluto realizzare questa guida sulla Sicurezza Informatica per illustrare ai propri Clienti le principali minacce e per fornire suggerimenti utili per difendersi dai crimini informatici.

Proteggere il Computer

Installare software antivirus e antispyware verificando che siano sempre aggiornati.
Utilizzare un firewall per evitare accessi non autorizzati al proprio computer.
Utilizzare aggiornamenti automatici (patch) del proprio sistema operativo. Le patch sono spesso in grado di riparare falle di sicurezza che possono lasciare i sistemi esposti alle minacce.
Effettuare il backup periodico dei dati presenti sul computer (documenti, immagini, etc.) per evitare che in caso di contagio da virus possano andare persi.

Utilizzare Password Sicure

Utilizzare password lunghe che contengano cifre, caratteri di punteggiatura, simboli e lettere maiuscole e minuscole in questo modo saranno più difficile da decifrare o dedurre provando tutte le possibili combinazioni.
Evitare di utilizzare parole, sostantivi, nomi propri o geografici contenuti nei dizionari.
Evitare di utilizzare informazioni personali che possono essere recuperate via internet (data di nascita, nome del partner o dei figli, numero di telefono, etc.).
Utilizzare password diverse per ciascun account in modo che, se anche un hacker riuscisse a decifrare una delle vostre password, sarà un solo account a essere violato

Acquisti Online

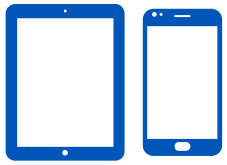
Evitare di effettuare acquisti da link contenuti in messaggi online non protetti, come ad esempio e -mail, post pubblicati su social media o messaggi istantanei.
Leggere, prima di acquistare, le recensioni degli utenti sui siti dove volete acquistare per verificarne l'affidabilità.
Effettuare acquisti solamente tramite siti Web che prevedono l'uso della cifratura. Il collegamento inizierà con "https://" (la "s" sta per "secure", ovvero "protetto") invece di "http://".
Cercare anche l'icona a forma di lucchetto nella barra di stato del browser.
Controllare gli estratti conto bancari, soprattutto dopo aver effettuato acquisti tramite Internet, per verificare che tutti i pagamenti indicati siano legittimi.

Phishing

Diffidare dalle e-mail che richiedono password e coordinate bancarie o che includono link per effettuare tali operazioni. Solitamente non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici, aggiornamento archivio, ecc.). Le banche non spediscono messaggi di questo genere.
Evitare di selezionare i link presenti nei messaggi di posta indesiderata. I phisher possono utilizzare questi link per reindirizzare l'utente su un sito Web fittizio. Meglio digitare l'indirizzo del sito nell'apposita barra per navigare all'interno della pagina autentica.
Inoltrare qualsiasi e-mail sospetta all'organizzazione direttamente coinvolta. Molte aziende hanno un indirizzo di posta creato appositamente per le segnalazioni di questo tipo.

Spamming

Installare un filtro antispam per evitare di ricevere messaggi di posta elettronica indesiderati o non richiesti.
Utilizzare due indirizzi e-mail: uno principale per le attività più importanti (Servizi bancari, rapporti con le Istituzioni, etc.) ed uno secondario per attività meno importanti (registrazioni su siti on-line, partecipare a sondaggi, etc.)
Evitare di pubblicare apertamente l'indirizzo e-mail sui social network (Facebook, LinkedIn, ecc...).
Evitare di utilizzare un indirizzo e-mail facilmente deducibile, contenente nome, cognome ed altri dati personali.



Dispositivi Mobile

Scaricare le app solamente dagli store ufficiali come Google Play Store e App Store di Apple.
Controllare le autorizzazioni richieste dalle applicazioni diffidando delle app che richiedono l'accesso a funzioni del sistema che non sembrano avere molto a che vedere con gli scopi dell'app stessa.
Tenere il sistema operativo e le app sempre aggiornate e installare un software antivirus.