# LA SICUREZZA IN INTERNET

E' sicuramente l'aspetto più rilevante alla base delle nuove tecnologie e delle applicazioni che sostengono il Web e che ne determinano in modo sostanziale il successo ed il livello di diffusione.

E' un tema assai dinamico anche per il costante adeguamento ai tentativi di frode ed articolato negli aspetti che coinvolge e che cercheremo di approfondirne senza entrare in tecnicismi poco comprensibili e soprattutto nell'ottica dell'uso corrente che di queste opportunità si può fare.

Ci focalizzeremo, pertanto, sui principali aspetti cercando di fornire utili suggerimenti:

- La sicurezza degli apparati;
- La sicurezza dei dati;
- La sicurezza dei siti;
- La sicurezza dei pagamenti.

## CONSIGLI PER LA SICUREZZA DEGLI APPARATI

- Aggiornare costantemente il sistema operativo e gli applicativi (App) di computer e smartphone scaricando solo gli aggiornamenti ufficiali presenti sui siti dei produttori; per le applicazioni da installare su smartphone far riferimento agli store ufficiali: Google Play per Android e Apple Play per IOS;
- Proteggere l'apparato con password, PIN o sistemi di riconoscimento biomedico (impronta digitale,riconoscimento facciale …);
- Installare adeguati software di protezione ( antivirus, firewall …) tenendoli costantemente aggiornati; ad esempio sui dispositivi Android è disponibile, gratuitamente, il servizio Google Play Protect per la protezione contro malware ed app dannose; l'abilitazione di questa funzione si può verificare avviando: Google Play>menù>Play Protect;
- Disattivare sullo smartphone wi-fi, bluetooth e geolocalizzazione quanto non li usi;
- Fare attenzione ad email che invitano a scaricare ed eseguire programmi di cui ignori la provenienza ;
- Diffida di email provenienti da indirizzi di istituzioni/aziende pubbliche/private che invitano a fornire dati personali per presunte problematiche; controllare l'indirizzo di provenienza e se non coincide con quello dei siti ufficiali spostare detti indirizzi tra le Spam (spazzatura);
- Le precedenti anomalie ed i tentativi di frode si possono segnalare alla Polizia Postale che ha un'apposita organizzazione per contrastare questi eventi;
- Controllare periodicamente le applicazioni installate sullo smartphone e se si riscontrano alcune non riconosciute e non desiderate negare ogni accesso ai dati (eventualmente richiesti) e disinstallarle immediatamente.

# CONSIGLI PER LA SICUREZZA DEI SITI

- Per navigare in internet utilizzare un motore di ricerca (browser) tra i più famosi quali Google Chrome, Firefox, Safari;questi operatori pongono una costante attenzione al problema delle frodi e delle violazioni di sistema ed, in genere, aggiornano automaticamente i propri prodotti sugli apparati d'utente ove sono installati; potrebbe essere utile consultare il link: arenzulla.it/google-chrome-amore-a-prima-vista-7760.html
- Verificare (anche nell'ipotesi di cui sopra) periodicamente l'aggiornamento del browser rilevando la versione installata; potrebbe essere utile consultare il link: arenzulla.it/come-aggiornare-browser-94800.html;
- I più famosi siti come Google Chrome inviano una segnalazione dei siti non sicuri del tipo
    - Il sito che stai per visitare contiene malware
    - Il sito che stai per visitare contiene programmi dannosi
    - Sito ingannevole
    - Questa pagina sta tentando di scaricare script da fonti non riconosciute
- Nel caso che dette notifiche non vengono attivate si può sempre accertare l'attendibilità del sito verificandone in autonomia la presenza del protocollo HTTPS che garantisce una comunicazione all'interno di una connessione criptata;si possono installare estensioni per browser che consentono di verificare l'attendibilità di un sito internet ( ad esempio per Google chrome: WOT: Web Of Trust);
- Installare un buon antivirus indispensabile per la navigazione online e per scaricare programmi;
- Quando si ha necessità di utilizzare la rete in assoluta riservatezza si può navigare in incognito con tecniche un po' conplicate.


# CONSIGLI PER LA SICUREZZA DEI PAGAMENTI

Il sistema dei pagamenti attraverso carta di credito è assolutamente sicuro sia dal punto di vista del consumatore che del venditore.

Il consumatore è completamente tutelato dall'istituto bancario emittente la carta contro ogni rischio di frode su tutti i suoi pagamenti online; nessuna responsabilità e nessun addebito per gli utilizzi illeciti della sua carta di credito.

Detti istituti hanno un servizio interno di controllo della carta verificando con il cliente eventuali usi anomali rispetto a griglie di controllo predefinite e, quando necessario, bloccano direttamente la carta stessa.

In caso di addebiti impropri il titolare della carta di credito ha 60 giorni, dal ricevimento dell'estratto conto, per inviare contestazione alla banca di emissione al fine di ottenere il rimborso sul proprio conto corrente.

Chi decide di vendere online deve considerare la sicurezza dei pagamenti online come uno dei principali fattori di successo ed utilizzare appositi sistemi.

Il pagamento online è, infatti, garantito da diversi sistemi di sicurezza che, avvalendosi di tecnologie di crittografia, garantiscono la sicurezza e la privacy della transazione online.

I principali sistemi sono:

- Il protocollo SSL (Security Sockets Layer) ; è il più diffuso prodotto commerciale che consente di realizzare un canale sicuro a livello di trasporto tra due elaboratori connessi ad internet;
- Il protocollo SET (Secure Electronic Transaction) sviluppato da Visa è Mastercard e prevede la codifica crittografata dei dati relative alla carta di credito prima del loro invio, per evitare possibili intercettazioni, e l'autenticazione dei soggetti che prendono parte alla transazione (titolare della carta, venditore e banca);
- Il sistema di sicurezza realizzato dai PSP (payment Service Peoviers), ossia i gestori di pagamenti elettronici per siti e-commerce,che offre all'esercente la possibilità di convenzionarsi tramite ls propria banca ed al consumatore di convenzionarsi/registrarsi per ottenere un portafoglio virtuale (wallet) nel quale inserire le proprie carte di credito; il consumatore si identifica al sistema tramite una password e non deve inserire i dati della carta che vuole usare ma solo indicare quale.

APPROFONDIMENTO: COSA SONO I PSP.

Un Payment Service Provider (PSP) è un soggetto che offre servizi online ad enti, negozi e commercianti per accettare pagamenti elettronici con una varietà di metodi di pagamento, tra cui carta di credito e pagamenti bancari quali addebito diretto, trasferimento etc.

Un PSP si connette a più banche (convenzionate), cards e sistemi di pagamento e, generalmente, gestisce completamente le connessioni tecniche, i rapporti con la rete esterna e i conti bancari nonché della procedura tecnica dei metodi di pagamento per i negozi online.

Dal punto di vista dell'acquirente si ha il vantaggio di non dover trasmettere nella transazione commerciale i dati della propria carta ma registrarli una sola volta presso il PSP; dal punto di vista del venditore si acquisisce una maggior libertà dagli istituti finanziari oltre a poter usufruire di ulteriori servizi che il PSP offre, quali: gestione del rischio, corrispondenza dei pagamenti, rendicontazione, fondi rimessa, servizi multi-valuta e protezione dalle frodi.

Le commissioni del servizio fornito da PSP sono addebitate direttamente ed esclusivamente al venditore; totalmente gratuite per l'acquirente.

Ci sono più di 900 fornitori di servizi di pagamento nel mondo, 300 in Europa; i più noti sono:

- Pay Pal
- Apple Pay
- Google Pay
- Satispay
- Ingenico
- Square

# LA SICUREZZA DEI DATI

Proteggere i propri dati o, se si è un operatore commerciale, i dati dei propri clienti è di importanza fondamentale quando si approccia il mondo della rete; non entriamo nel merito del commerciante con problemi complessi di protezione degli apparati e della propria rete Wi-Fi, limitandoci al tema dell'utilizzatore privato della rete fornendo alcuni consigli pratici:

- proteggi il tuo smartphone o tablet con password/PIN e se possibile con sistemi di riconoscimento biometrico (impronta digitale, riconoscimento del volto, …); imposta una password sicura per accedere alla rete; utilizza password differenti per accesso alla rete e ai tuoi dispositivi e non salvarle mai sul tuo dispositivo; modifica periodicamente la password.
- installa e mantieni sempre aggiornato il software di protezione antivirus e antispyware ; installa un firewall personale ; il software antivirus permette di tenere il proprio dispositivo al riparo da software indesiderati ("malware") che potrebbero essere installati senza il consenso dell'utente.
- installa tempestivamente gli aggiornamenti e patch ufficiali del Sistema Operativo e dei principali programmi che usi

- elimina periodicamente i cookies e i file temporanei Internet utilizzando le opzioni del tuo browser
- effettua regolarmente scansioni complete con l'antivirus
- non installare applicazioni scaricate da siti non certificati o della cui attendibilità non sei sicuro; in fase di installazione, fai attenzione ai permessi richiesti assicurandoti che siano strettamente connessi al servizio che intendi utilizzare
- se lo stesso PC è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole ;
- ricorda di disattivare Wi-Fi, geolocalizzazione e bluetooth quando non li usi ;
- attiva, quando possibile, le funzionalità di "remote lock" e "remote wiping", che ti consentiranno, in caso di furto, di bloccare e cancellare i dati contenuti sul tuo dispositivo mobile da un altro PC.

## ANNOTAZIONI

COME PRETEGGERSI DAL PHISHING: Il phishing è una tipologia di frode informatica che si realizza tipicamente mediante la creazione di siti internet fraudolenti rassomiglianti, nei contenuti e nella grafica, a quelli di aziende note, cui l'utente viene invitato a collegarsi tramite invio di false e-mail o sms, convincendolo a fornire informazioni personali, dati finanziari o codici di accesso. Ecco alcuni preziosi consigli per identificare un tentativo di Phishing:

- Controlla l'indirizzo email del mittente; tipicamente i pirati informatici utilizzano degli indirizzi di posta elettronica che sembrano essere quelli ufficiali, ma in realtà differiscono anche solo di una lettera; prima di cliccare su di un link presente in una email, accertati che la e-mail arrivi veramente da un mittente ed un indirizzo ufficiale.
- Analizza il testo della comunicazione; fai attenzione alle comunicazioni che presentano errori ortografici e grammaticali o fanno un uso scorretto della lingua italiana; probabilmente sono mail di phishing; diffida da mail contenenti messaggi con toni intimidatori e con carattere d'urgenza che ti chiedono la verifica di dati personali o di Carta di Credito.
- Controlla l'indirizzo del sito internet evitando di cliccare su link che rimandano a siti bancari se all'interno di email o SMS sospetti; le email di phishing fanno inoltre uso di URL abbreviate (short URL) per nascondere indirizzi web non legittimi; non aprirle e verifica che il sito web a cui accedi sia caratterizzato dalla presenza dell'"https", a garanzia dell'utilizzo di protocolli sicuri di comunicazione;
- Verifica che sia presente il lucchetto verde nel browser, cioè che il sito sia certificato e sicuro; un sito sicuro e certificato adotta i protocolli di sicurezza per la gestione dei dati, assicura l'integrità dei dati e garantisce comunicazioni cifrate tra il tuo dispositivo e il servizio a cui ti connetti.

ATTENZIONE AL VISHING : Il vishing è una forma di phishing basata sull'uso del telefono. Viene richiesto, tramite email o SMS, di chiamare un numero telefonico al quale comunicare i

propri codici identificativi (Username/Email e Password). In alternativa, viene effettuata una chiamata preregistrata, in cui viene chiesta l'immissione e conferma dei codici identificativi.

PASSWORD SICURA: una password costituita da frasi o parole facilmente intuibili è a rischio; ecco qualche consiglio per creare una password sicura e facilmente memorizzabile:

- Crea la tua password componendola con le iniziaòi di una frase che possa ricordare soltanto tu e non associabile ai tuoi dati anagrafici; ad esempio: QEAIVS (Questa Estate Andrò in Vacanza in Sardegna ), UMAGLM (Una Mela Al Giorno Leva il Medico); una strofa di una canzone o di una poesia sono ottimi esempi. Invece il tuo nome, la tua data di nascita o quella di un tuo caro sono intuibili e non sicure;
- Usa combinazioni di caratteri alfanumerici con maiuscole /minuscole, simboli speciali (QeArf26&);
- Evita di utilizzare parole di senso comune o riferite alla tua vita privata o aziendale; ad esempio: nomi propri, codice fiscale, date di nascita, targa auto …)

SISTEMA DI RICONOSCIMENTO BIOMETRICO : è un particolare sofware che ha la funzionalità e lo scopo di individuare una persona sulla base di caratteristiche biologiche e/o comportamentali (biometria) confrontandole con i dati precedentemente acquisiti e memorizzati nel data base del sistema.

Le caratteristiche prese in considerazione possono essere di tipo fisiologico ( impronte digitali, colore e dimensione dell'iride, le retina, il volto o parti di esso …) o ti tipo comportamentale (impronta vocale, scrittura grafica, la firma …).

I sistemi di riconoscimento biometrico vengono utilizzati in diversi tipi di mercato, sia in ambito governativo (Militare, Sanità, Giustizia, enti e istituzioni pubbliche) e sia in quello commerciale (turismo, trasporti, banche, assicurazioni, hi-tech, telecomunicazioni, industria), per assicurare una maggiore sicurezza ai sistemi, alle transazioni e alla tutela dei dati. Le applicazioni maggiormente in uso sono:

- autenticazione degli accessi fisici in locali protetti,
- sicurezza nelle transazioni finanziarie,
- prevenzione delle frodi,
- proteggere e tutelare l'attività bancaria via internet,
- identificazione di soggetti,
- sicurezza negli aeroporti,
- investigazione,
- schedatura dei criminali.
- identificazione e schedatura delle persone migranti

Un particolare campo di applicazione dei sistemi di riconoscimento biologico sono gli **smartphone**, in particolare il sistema più diffuso è il riconoscimento dell'impronta digitale tramite un apposito lettore che permette di sbloccare il proprio cellulare appoggiando il dito di cui si è registrata l'impronta, metodo spesso preferito dagli utenti perché più veloce rispetto all'inserimento della sequenza o della password. Nel 2017 vengono introdotte due nuove tipologie di riconoscimento biometrico: uno da parte di **Apple**, la quale ha introdotto un sistema di riconoscimento facciale sull'iPhone X chiamato Face ID ed un altro da parte di **Samsung**, un sistema di riconoscimento basato sulla scansione dell'iride.