sogei

Web consapevole

Guida per un utilizzo consapevole della rete

WEB CONSAPEVOLE

Sommario

1. Identità digitale

1.1 Creazione di password complesse

Le password fanno ormai parte della vita quotidiana, da quando si accede alla posta elettronica a quando si effettuano acquisti on-line. Le password robuste sono un elemento essenziale per la protezione dei dispositivi; password semplici, infatti, possono essere carpite consentendo ad estranei di avere accesso alle informazioni personali nonché ad effettuare operazioni sensibili come, ad esempio, trasferire del denaro.

Ci sono alcuni accorgimenti che è bene adottare per migliorare la sicurezza delle password in modo da proteggere account, dispositivi fisici e operazioni online.

Innanzitutto, è bene impiegare una password differente per ogni account. Meglio non scegliere una password sola e usarla ovunque: se un hacker se ne impossessa, la proverà su tutti i siti web ai quali ci si è registrati per carpire quante più informazioni possibili.

Non utilizzare password banali ma creative; scegliere nome, cognome e data di nascita non è mai una buona idea. Anche adoperare una singola parola di senso compiuto, soprattutto se corta, può compromettere la sicurezza degli account personali.

Una password robusta deve avere anche le dimensioni giuste; la lunghezza di almeno quattordici caratteri è una caratteristica auspicabile, ma deve essere accompagnata da un certo livello di complessità. Una buona strategia potrebbe essere quella di combinare lettere (maiuscole e minuscole), numeri, simboli e segni di punteggiatura, se permessi. Una password del genere potrebbe essere ottenuta mettendo assieme le iniziali di una frase.

C'è però un rovescio della medaglia; password lunghe e complesse possono essere difficili da ricordare per cui è ancora meglio utilizzare delle passphrase, in altre parole delle semplici frasi, facili da ricordare ma difficili da indovinare. Per la costruzione di una valida passphrase valgono le stesse indicazioni: non conta solo la lunghezza ma anche la combinazione di lettere maiuscole, minuscole e simboli (compresi gli spazi). Si può rendere la passphrase ancora più robusta sostituendo lettere con numeri o simboli, ad esempio la lettera "e" con il numero "3" o la lettera "l" con il punto esclamativo.

È bene ricordare, quindi, che una password tradizionale può essere più facilmente indovinata da un hacker o violata con strumenti progettati ad hoc. Le passphrase, invece, sono molto più difficili da violare perché la maggior parte di questi strumenti non è efficace avendo messo in pratica tutti questi suggerimenti.

Se si dispone di molti account può essere difficile ricordare tutte le password o passphrase; una soluzione consiste nell'utilizzo di un password manager, cioè un'applicazione progettata per conservare in modo sicuro le proprie credenziali. I password manager memorizzano questi dati e li proteggono con una password o passphrase, denominata master password, che sarà necessaria

per recuperare le credenziali di accesso degli account personali: è fondamentale che la master password sia robusta perché rappresenta la combinazione della propria “cassaforte digitale”. Esistono svariati password manager sia gratuiti che a pagamento che forniscono inoltre indicazioni sul livello di sicurezza delle password degli account personali. I password manager possono funzionare sia nel cloud, avendo quindi sempre a disposizione le proprie password, sia come archivio locale, e sono disponibili sia per pc che via web o tramite app per smartphone.

Come per tutti i software, è necessario assicurarsi di tenere aggiornata l’app di password manager sui propri dispositivi.

1.2 Difesa dalle frodi

La posta elettronica è uno dei principali strumenti di comunicazione ed è anche uno dei modi con cui le aziende forniscono servizi online, ad esempio la conferma di un acquisto o di un bonifico effettuato. Per questo motivo è diventato uno degli strumenti di attacco più utilizzati da criminali e truffatori per la frode nota come *phishing*; email e servizi di messaggistica, come ad esempio quelli dei social network, sono impiegati come esca, con lo scopo di ingannare e convincere il destinatario a compiere un’azione, ad esempio cliccare un link o aprire un allegato.

Cadere vittima di questi attacchi provoca il furto di informazioni sensibili o la compromissione dei dispositivi, computer o smartphone, attraverso l’installazione di software chiamati *malware*. I truffatori, per rendere le loro email o messaggi verosimili, fanno in modo che sembrino provenire da un conoscente, un amico, o dalla banca (con tanto di logo) e cercano di indurre ad aprire un allegato oppure a cliccare un link che conduce a un sito civetta, con le sembianze di quello originale: tutti i dati inseriti (username, password, codici di accesso, etc..) saranno però inviati ai criminali!

È bene ricordare, quindi, che allegati e link contenuti in tutte le email vanno trattati con cautela; se si nutrono dei sospetti, si può ad esempio portare il mouse su di essi, senza cliccare, e verrà mostrato il collegamento reale. Se i due link non corrispondono, si tratta molto probabilmente di un tentativo di phishing ed il messaggio deve essere cancellato. In caso di dubbi, ignorare la mail e collegarsi direttamente al sito della banca o della società che ha scritto, lì sono disponibili tutte le informazioni necessarie.

Inoltre è necessario prestare molta attenzione agli allegati, soprattutto se inattesi, e se il messaggio chiede con urgenza di aprirli; esempi di questo tipo sono le comunicazioni provenienti dalla banca, da un’istituzione della pubblica amministrazione o da un sito web di acquisti online. Accedendo all’allegato si scatenerà un attacco capace di impedire l’accesso a tutti i dati personali! È consigliabile utilizzare sempre un software antivirus aggiornato e contattare, quando possibile, il mittente del messaggio attraverso un altro canale prima di aprire qualsiasi tipo di allegato.

Attenzione infine ai siti web che mostrano finestre o pop-up contenenti avvisi relativi alla presenza di virus o altri problemi di sicurezza nel sistema, che invitino a visitare una pagina da cui scaricare una soluzione antivirus. Si tratta ovviamente di una truffa perché il software è in grado di rubare i dati personali; infatti, nessun fornitore affidabile di software antivirus impiega queste tattiche allarmistiche; se i messaggi non provengono da un programma precedentemente installato, attenzione a non fare clic su nessuno di essi.

1.3 Politiche di privacy

Il diritto di impedire che le informazioni personali siano trattate da altri, senza aver volontariamente espresso il consenso, è di estrema importanza: la privacy è un diritto inviolabile, posto a garanzia del fatto che ciascuno possa scegliere di esprimere ciò che è, nel rispetto delle libertà altrui.

La normativa italiana disciplina il trattamento dei dati personali e prevede sanzioni severe per chi non rispetta le disposizioni. Ogni sito internet deve quindi essere dotato di una politica di privacy, che informi quali dati personali saranno registrati (dietro esplicito consenso), a cosa servano queste informazioni e come si intende utilizzarle. È quindi buona abitudine consultare la sezione relativa alle politiche di privacy e valutarne l'adeguatezza, prima di iniziare a utilizzare i servizi offerti da qualsiasi sito web.

Attenzione inoltre ai messaggi con cui i siti web informano sull'utilizzo di cookie: si tratta di piccoli file di testo che gli stessi inviano al computer, tablet o smartphone. Alcuni cookie sono utilizzati per motivi tecnici e sono indispensabili per eseguire operazioni che, in loro assenza, risulterebbero molto complesse o meno sicure, mentre altri sono utilizzati per tracciare la navigazione in rete e creare profili basati sui gusti, abitudini e scelte personali. Grazie a questi cookie possono essere trasmessi messaggi pubblicitari in linea con le preferenze già manifestate nel corso della navigazione online: i siti web che intendono farne uso sono tenuti a comunicarlo appena vengono visitati e a richiedere esplicitamente il consenso. È prevista inoltre una pagina di informativa estesa in cui è possibile reperire maggiori e più dettagliate informazioni sui cookie e scegliere quali autorizzare attraverso le impostazioni del browser.

In generale, conviene sempre evitare di fornire informazioni personali che non siano necessarie; per iscriversi a una piattaforma elettronica, un social network o altro, una scelta prudente è quella di compilare i soli campi obbligatori, contrassegnati con un asterisco.

Il Codice in materia di protezione dei dati personali riconosce vari diritti nei confronti del titolare del trattamento dei dati, indicato dalla politica di privacy di ogni sito web, tra cui:

- l'accesso ai propri dati
- l'aggiornamento, la rettifica o l'integrazione
- la cancellazione, la trasformazione in forma anonima o il blocco

- l’opposizione al trattamento effettuato a fini promozionali, pubblicitari o commerciali

Per esercitare questi e gli altri diritti previsti dal Codice occorre presentare un’istanza allo stesso, senza particolari formalità.

2. Social network

Questa sezione offre consigli utili su come sfruttare le potenzialità della rete e dei suoi strumenti e servizi, sia mediante un utilizzo più consapevole che cercando di evitare pericoli, rischi e insidie che possono nascondersi, come nella vita reale, anche nel mondo virtuale.

2.1 Utilizzo sicuro dei social media

I social media sono uno strumento fondamentale, da tempo presente nella vita quotidiana e che probabilmente sarà presente ancora per molto anni futuri, nelle varie incarnazioni ed evoluzioni. La caratteristica fondamentale è quella di mettere in comunicazione le persone, tenere contatti con chiunque si voglia ed avere notizie in tempo reale da qualunque parte del mondo.

Questa potenzialità enorme, che crea appunto un'unica rete di persone globale e che ha, di fatto, cambiato le abitudini sociali in pochi anni, presenta diversi rischi connessi alla sua natura.

Il rischio principale che ogni utente deve affrontare quando usa un social network è molto ben sintetizzato dalla parola inglese *oversharing*. Il diffondere troppe informazioni è appunto la cosa più pericolosa che può succedere utilizzando un servizio che, per sua natura, permette di pubblicare un contenuto leggibile potenzialmente, ovunque nel mondo e da chiunque. Senza contare che tutti i dispositivi personali hanno un rilevatore GPS, e quindi basta un clic per far sapere a chiunque, magari anche con cattive intenzioni, che si è assenti da casa ma ad esempio in vacanza a chilometri di distanza.

I filtri privacy presenti sui vari servizi sono sicuramente un ottimo punto di partenza ma il filtro principale non può non essere quello presente nella nostra testa. Un contenuto diffuso tramite social network è, per sua definizione e comunque perché "digitale", un contenuto del quale non avremo più controllo una volta inviato. Poco importa che si invii a due o a cento persone, la sua natura intrinsecamente replicabile (basta un clic) lo porta ad avere una potenziale diffusione che potrebbe andare oltre ogni nostra più pessimistica valutazione.

Ad esempio una foto inviata, magari con richiesta di riservatezza, a un nostro contatto in chat, può essere inoltrata da questo stesso contatto, con due clic, su un gruppo magari con decine di altre persone. E questo può essere fatto sia con volontà da parte sua, sia soprattutto involontariamente, magari perché si pensava di inviare un'altra cosa.

Questa leggerezza rischia di causare danni molto gravi che potrebbero avere un impatto negativo sia nella vita privata che nella carriera professionale.

Una rete sociale di interconnessione è quindi sì uno strumento incredibile che ci permette di essere in contatto in tempo reale con chiunque, però proprio per questo e proprio per il fatto che il digitale permette una replicabilità immediata con un'ampiezza enorme, va ricordato sempre che il primo filtro privacy siamo noi.

Se ci viene il dubbio che un contenuto, una foto, una frase o un luogo, non debba stare su un social network, probabilmente faremmo bene a non pubblicarlo.

2.2 Attenzione alle truffe online

I truffatori operano da sempre con un unico scopo: cercare di prendere soldi dalla vittima facendo credere di vendere chissà quale tipo di beni e servizi. Dal mondo reale a quello digitale la situazione è analoga, con dei rischi maggiori da un lato e con degli strumenti più efficienti dall'altro.

I rischi sono dovuti al fatto che manca l'intermediazione tra le persone che spesso (ma non sempre) è una chiave per poter prevenire possibili truffe. Nel caso dello shopping poi manca proprio la visione dell'oggetto della trattativa che quindi può essere spacciato per qualunque cosa.

Il vantaggio è sicuramente dato dalla possibilità di leggere le recensioni di altri utenti su un venditore o un fornitore di servizi (ad esempio di un sito di aste online o di un ristorante) così da avere un riscontro prima di avviare una transazione.

2.3 Shopping online senza rischi

Nell'ambito delle truffe online, gran parte dei rischi che si presentano sono la riproposizione di quanto già avviene nel mondo reale. Il maggior numero di clonazioni di carte di credito, ad esempio, avviene fuori da internet con POS manomessi o con *skimmer* (dispositivi in grado di leggere e immagazzinare i dati di una carta) applicati fisicamente ad un bancomat per strada.

Sul web si aggiunge la mancata intermediazione fisica tra due persone. Quello che però non cambia è il concetto di fiducia che deve sempre essere presente quando c'è una transazione di denaro. Se un negozio o un venditore non dà affidamento, si evita di acquistare; allo stesso modo è bene comportarsi online: se un sito non sembra attendibile o chiede troppe informazioni personali, forse è il caso di soprassedere.

Grandi negozi online spesso offrono garanzie di sicurezza maggiori rispetto ad un sito di e-commerce poco noto o ospitato su server poco sicuri, così come comprare in un grande magazzino è sovente garanzia di maggior qualità e sicurezza rispetto ad un banchetto per strada.

I modi principali di proteggersi sono diversi. Si possono utilizzare strumenti finanziari avanzati, come ad esempio carte ricaricabili o virtuali, cioè con la cifra esatta che si vuole spendere o addirittura con un codice usa-e-getta che renda la carta usabile una volta sola. In questo modo in caso di furto dei dati della carta non si potrà perdere nulla oltre alla cifra stanziata.

Un altro sistema è affidarsi a un intermediatore di pagamenti che garantisca i trasferimenti di valuta e tracci ogni transazione. Questo significa dare il proprio numero di carta solo a queste aziende che solitamente hanno sistemi di sicurezza molto elevati e pagare tramite loro. In questo modo il venditore avrà solo i dati della transazione e del cliente, ma non vedrà mai il numero della carta.

Spesso questi stessi servizi offrono anche protezione in caso di mancata spedizione dell'oggetto acquistato o di problemi nella stessa.

Va ricordato poi che nella legislazione italiana è presente il Diritto di Recesso, che permette a un consumatore di restituire l'oggetto entro quattordici giorni e avere indietro la somma spesa.

Sempre parlando di fiducia, un sito che dettaglia bene e chiaramente le modalità con cui l'acquirente può esercitare questo diritto è sicuramente segno di serietà e affidabilità.

Come per la Privacy, vale sempre il discorso che lo strumento di difesa più efficiente sia l'utente stesso: nel caso di dubbi, o magari di offerte che sembrano troppo vantaggiose o convenienti, è meglio evitare e magari rivolgersi a chi ha un'affidabilità più alta.

2.4 Rischi per i minori

I nativi digitali, cioè le persone che sono nate e cresciute quando l'infrastruttura di internet già esisteva, hanno da un lato una facilità di uso e una assimilazione innata di questi strumenti, dall'altro però, non avendo seguito il loro sviluppo e la loro progressiva introduzione, possono non comprendere a fondo i rischi e i dubbi che emergono nell'usare questi strumenti molto potenti e molto utili.

Uno dei problemi più seri è la mancanza di intermediazione fisica tra le persone. I genitori spendono tanta energia e fatica a far comprendere ai figli di non frequentare le "cattive compagnie", che nella vita reale sono (a torto o a ragione) identificabili fisicamente.

Online le cose cambiano perché è estremamente facile sembrare qualcun altro, e questo, unito appunto ad una fiducia innata in uno strumento che i ragazzi hanno sempre visto come parte delle loro vite, porta a sottovalutare il problema e a non valutare adeguatamente i rischi

Fondamentale è, quindi, da parte degli adulti un insegnamento al dubbio: così come si insegna ad essere cauti nel fornire informazioni personali ad estranei, lo stesso comportamento si deve adottare quando si naviga in rete, anche se l'estraneo sembra essere, dall'immagine del profilo pubblicata, un compagno di scuola o un coetaneo.

Capita spesso però, anche agli adulti, di non dare la giusta attenzione ai consigli nella sezione dedicata sui social network. Può accadere, infatti, che si condividano troppe informazioni, senza valutare attentamente i rischi connessi.

Un esempio è il primo giorno di scuola, momento in cui i social network si riempiono di foto di bambini davanti ai cancelli. Chi pubblica non si rende conto che sta fornendo informazioni sul minore, su qual è la scuola frequentata e magari anche la classe. Spesso questi post sono geolocalizzati e pubblicati senza appropriati filtri privacy, rendendo così molto semplice individuare il minore, magari spacciandosi come amico di famiglia.

Il consiglio utile, sia agli adulti che ai ragazzi, è di riflettere prima di condividere informazioni perché, come e più che nella vita reale, nel mondo virtuale non si sa mai chi sono gli interlocutori.

3. Protezione dei dispositivi

I criminali informatici sono costantemente alla ricerca di nuove debolezze nei sistemi operativi e nelle applicazioni; per questo motivo i produttori distribuiscono periodicamente degli aggiornamenti in modo da porvi rimedio. Aggiornare i dispositivi significa quindi renderli più sicuri; assicurarsi quindi di attivare gli aggiornamenti automatici in modo che sia sempre disponibile l'ultima versione del sistema operativo o delle applicazioni installate.

Questa regola si deve applicare a ogni apparato connesso alla rete, inclusi i dispositivi TV collegati a Internet, i monitor per i neonati, i router di casa e le console di gioco. Quando si acquista un dispositivo nuovo o si reinstalla il sistema operativo non sempre si ha a disposizione un sistema dotato degli aggiornamenti più recenti: il primo passo da fare, a questo punto, è collegarsi a internet e scaricare gli aggiornamenti del sistema operativo; prima è bene assicurarsi di essere protetti da un antivirus e da un firewall. È buona norma abilitare il controllo degli aggiornamenti in modo che avvenga almeno una volta al giorno, per essere certi che il dispositivo sia sempre allineato alle ultime versioni e quindi più sicuro, e procedere all'installazione di quelli che richiedono un intervento per autorizzare l'operazione. Le novità introdotte da un aggiornamento possono essere generalmente lette nella "Nota di rilascio", visualizzata prima di procedere all'installazione: gli sviluppatori del software tendono sempre a migliorare il proprio prodotto, adeguandolo e ottimizzandone le prestazioni.

Se il sistema operativo dei personal computer, smartphone, tablet o altro non è più supportato e non è più in grado di ricevere aggiornamenti, si raccomanda di sostituirlo con una nuova versione.

3.1 Smartphone e tablet

Smartphone e tablet, così come i personal computer, sono strumenti utili a comunicare, fare acquisti online, giocare e molto altro. Sui dispositivi connessi alla rete è conservata una grande quantità di informazioni sensibili: ad esempio, documenti personali, immagini ed email. È quindi indispensabile adottare alcuni accorgimenti per proteggerli ed evitare che le informazioni contenute finiscano nelle mani sbagliate.

I personal computer, i tablet e gli smartphone possono essere smarriti o rubati: il primo passo da fare è quindi quello di abilitare il blocco dello schermo. In questo modo chiunque sia in possesso del dispositivo potrà accedervi solo se è a conoscenza del codice di sblocco o, ancora meglio, della password precedentemente impostata e che deve essere caratterizzata da un adeguato livello di complessità. Su alcuni modelli esistono le funzionalità di cancellazione dei dati, in caso di inserimento di un numero elevato di password errate, e di abilitazione della cifratura della memoria del dispositivo. In questo modo l'eventuale ladro non riuscirà ad accedere ai dati, anche provando a connettere il dispositivo direttamente ad un computer.

È bene prestare attenzione alle app installate su smartphone e tablet e applicazioni scaricate dal web sui vostri personal computer: scegliere solo quelle di cui si ha realmente bisogno e che provengono esclusivamente da fonti attendibili. Alcuni di questi software possono, infatti, nascondere al proprio interno programmi utilizzati dai criminali informatici per infettare computer e dispositivi mobili, comunemente indicati con il termine malware; altri strumenti che possono essere utilizzati per questo scopo sono allegati email, file scaricati attraverso il Web, ricevuti attraverso servizi di messaggistica o da supporti di memoria come pendrive.

Uno dei modi per proteggersi da queste minacce è installare un anti-virus proveniente da un produttore di fiducia. Questo strumento, chiamato anche anti-malware, è progettato per individuare e fermare il software nocivo che potrebbe altrimenti consentire a un hacker di catturare tutto ciò che si digita, rubare documenti ed immagini o usare il computer violato per attaccarne altri. Un anti-virus esegue una scansione dello smartphone, del tablet o del personal computer alla ricerca di malware conosciuti: nel caso in cui un file risulti infetto lo stesso sarà eliminato per neutralizzare la minaccia. Alcuni anti-virus per smartphone presentano anche funzionalità di protezione delle app, andando ad individuare app malevoli o che simulino app note.

I criminali informatici sviluppano però nuove e sempre più sofisticate soluzioni in grado di evitare i tentativi di individuazione, per cui i produttori di anti-virus provvedono ad aggiornarli costantemente con nuove caratteristiche: il miglior modo per difendersi dai pericoli è quindi quello di installarli non appena sono resi disponibili o di attivare la funzione di aggiornamento automatico. Se il dispositivo è offline o spento per un certo tempo, l'anti-virus avrà bisogno di aggiornarsi al momento dell'accensione: si consiglia di non ritardare in nessun caso questa importante operazione. Attenzione agli avvisi generati dall'anti-virus: molti di essi prevedono la possibilità di ottenere maggiori informazioni o raccomandazioni su cosa fare.

Un anti-virus non è infallibile perché i criminali informatici sviluppano nuovo malware così velocemente che i produttori non sempre sono in grado di individuare e bloccare tutti gli attacchi: è essenziale essere prudenti nell'installare applicazioni e nello scaricare file di qualsiasi tipo.

3.2 Personal computer

Personal computer, tablet e smartphone consentono di connettersi in modo semplice a Internet per utilizzarne i tanti servizi disponibili, come ad esempio navigare sul Web o accedere alla posta elettronica. I dispositivi possono scambiare informazioni con tutti gli altri connessi alla rete, tra i quali però ci sono quelli utilizzati dai criminali informatici: se non sono impiegati strumenti utili a contrastarli, è possibile che qualcuno riesca ad ottenere l'accesso al sistema personale.

È necessario mantenere alta l'attenzione non solo quando si utilizza la connessione rete domestica, ma soprattutto quando si è in movimento e ci si collega ad una nuova rete, come un hotspot Wi-Fi pubblico; in questo caso non c'è nessuna garanzia che sia sicura. Una buona abitudine è installare sui dispositivi un firewall personale che permetta di restringere gli accessi.

Un firewall funziona come un filtro che intercetta tutte le connessioni fra il dispositivo e internet e seleziona quali consentire e quali invece no; in questo modo riesce a impedire quelle non autorizzate e, in base a come è configurato, può bloccare dati sia in entrata che in uscita. Rende quindi estremamente difficile che qualcuno dall'esterno riesca a penetrare nel dispositivo protetto.

Quasi tutti i sistemi operativi includono già al loro interno un personal firewall, ma è raccomandabile installare e impiegare un firewall specializzato che offra maggiori funzionalità, sia sui personal computer che su tablet e smartphone; ne esistono anche ottime versioni gratuite, disponibili attraverso i canali ufficiali.

La maggior parte dei firewall è preconfigurata in modo da garantire un livello di sicurezza sufficiente; è però caldamente consigliata un'accurata lettura delle istruzioni di configurazione del produttore perché, se mal configurato, questo componente potrebbe anche bloccare funzionalità e software consentiti. È buona norma adottare inizialmente una configurazione meno restrittiva e in seguito, dopo aver acquisito maggiore dimestichezza, rinforzare le difese. Non preoccuparsi in caso il firewall invii avvisi circa le operazioni in corso; al contrario, questa è la prova che compie il suo lavoro correttamente. Quando un programma o un'app tenterà per la prima volta di inviare informazioni via internet o cercherà di collegarsi a un sito con lo scopo di prelevare o trasmettere dati, il firewall "metterà in attesa" il tentativo di accesso alla rete e provvederà a segnalarlo; è possibile scegliere tra tre possibilità, lasciandosi guidare dal buonsenso e dalla prudenza:

- bloccare la comunicazione di rete
- consentire la comunicazione di rete
- impostare una regola per i tentativi di accesso futuri

L'utilizzo combinato di un personal firewall e di un anti-virus aggiornato permetterà di proteggere i dati da occhi indiscreti, rendendo i propri dispositivi più sicuri da attacchi esterni.

4. Difesa dei dati

4.1 Utilizzo Cloud

Tra le nuove tecnologie affermatesi negli ultimi anni, quella più diffusa è il *cloud computing*, che offre servizi di gestione e conservazione dei dati online. Su internet esistono vari esempi di questo tipo come siti web che consentono l'archiviazione e la condivisione di file (immagini e documenti di vario genere).

I vantaggi di queste tecnologie sono molteplici, per esempio la possibilità di sincronizzare le informazioni su tutti i propri dispositivi o quella di condividere informazioni con chi si desidera. Tuttavia è necessario fare attenzione al fatto che in questo modo i dati privati non sono più solo conservati su dispositivi di proprietà, ma anche su computer, gestiti dai cosiddetti cloud provider, su cui non si ha alcun controllo.

Per questo motivo è bene adottare delle misure di sicurezza per proteggere i dati personali:

- scegliere fornitori che offrano servizi di facile utilizzo e comprensione; più questi sono complessi, più facilmente si possono compiere errori ed esporre o perdere accidentalmente i propri contenuti
- leggere i termini di servizio e verificare quali siano i propri diritti legali e chi possa avere accesso ai dati
- prestare attenzione al modo in cui si utilizza il cloud; come prima cosa assicurarsi che la password di autenticazione al servizio sia sufficientemente robusta

Alcuni tipi di servizi cloud offrono la possibilità di condividere file semplicemente attraverso un link da inviare alle persone cui si desidera distribuirli; è bene essere consapevoli che questo approccio non è sicuro in quanto consente di accedere ai file se a conoscenza del link. Una possibile contromisura consiste nel rimuovere il link quando non ce ne sarà più bisogno.

Attenzione inoltre a ciò che si condivide. Per non rischiare di rendere visibili su internet i dati personali, è buona norma impostare come regola predefinita quella che preveda nessuna condivisione, e scegliere poi, di volta in volta, quello che si vuole condividere con gli altri. Preferire i cloud provider che dispongono di un modo semplice per configurare i permessi di accesso e consultare chi ha acceduto a file e cartelle.

È possibile specificare successivamente quali persone o gruppi potranno accedere ai contenuti a loro riservati; ricordarsi di revocare il permesso quando questi non ne avranno più bisogno.

L'utilizzo del cloud si basa inoltre sulla fiducia che il fornitore sia sempre in grado di assicurare il servizio; tuttavia è bene prevedere un backup dei dati in caso questo non avvenga.

Avere un antivirus aggiornato sia sul proprio computer che sui dispositivi che si utilizzano per archiviare i dati sul cloud, eviterà che i file condivisi siano infettati e che quindi si possano involontariamente trasmettere virus a coloro che vi accedano.

4.2 Consigli utilizzo Wi-Fi

Nel corso degli ultimi anni il numero di reti Wi-Fi pubbliche è cresciuto notevolmente; accedervi può comportare dei rischi, come il furto dei propri dati e delle credenziali di accesso ai servizi online, se non si adottano alcune semplici precauzioni. Esiste inoltre la possibilità che la rete Wi-Fi aperta sia una trappola creata ad hoc proprio per rubare i dati di chi si connette.

Per fortuna bastano pochi accorgimenti per continuare a utilizzare le reti Wi-Fi pubbliche con maggiore sicurezza.

Attenzione quando si accede a reti wireless pubbliche, come ad esempio quelle che si trovano nei caffè o negli aeroporti, perché chiunque può controllare le attività svolte.

La prima e più importante contromisura consiste nel verificare l'attendibilità della rete a cui ci si connette; se si è in un esercizio pubblico, ad esempio, è buona norma chiedere al gestore il nome della rete Wi-Fi.

Nei luoghi pubblici fare attenzione alle reti aperte che non siano ricollegabili a un soggetto identificabile; il rischio è che sia una rete creata ad hoc per rubare i dati di chi si connette.

Ecco perché in questi casi è consigliabile assicurarsi che le comunicazioni personali siano protette da crittografia, che rende impossibile la comprensione a chi le intercetta. Ad esempio, quando ci si collega a internet con un browser, assicurarsi che i siti visitati siano protetti; in questi casi nella barra degli indirizzi sarà presente l'immagine di un lucchetto chiuso. Una scelta prudente è quella di non utilizzare una rete Wi-Fi pubblica per collegarsi alla propria banca o effettuare acquisti online e, più in generale, quando le informazioni trasferite si ritiene siano sensibili.

Smartphone, tablet e personal computer potrebbero connettersi in automatico a una Wi-Fi pubblica; in questo caso non si ha modo di impedire la connessione a una Wi-Fi trappola. Per proteggersi da questo tipo di rischio è importante disattivare l'accesso automatico alle reti Wi-Fi conosciute.

Se si teme che non ci siano punti di accesso Wi-Fi affidabili, si possono attivare le funzionalità di tethering o hotspot sul proprio smartphone.

Una buona abitudine è installare sui dispositivi un firewall personale utile come filtro che intercetti e selezioni tutte le connessioni fra il proprio dispositivo ed internet. In questo modo si riescono a impedire le connessioni non autorizzate e, in base alla configurazione scelta, si possono bloccare i dati sia in entrata che in uscita.

Via Mario Carucci, 99 e 85 - 00143 Roma
Tel. 06.50251 - Fax 06.50526289
www.sogei.it