con la partnership scientifica di:

Unità 5

Garantire la sicurezza

Livello 3 - approfondimento

Temi trattati all'interno dell'Unità

- Introduzione alla sicurezza.
- Il fattore umano (Il Social Engineering).
- Controllo degli Accessi: Identificazione, autenticazione, crittografia e non ripudio
- La sicurezza dell'informazione
- Uso della Crittografia
- Crimini digitali: i principali tipi di attacco e consigli di protezione

Sommario

IL FATTORE UMANO E Il SOCIAL ENGINEERING 1

LA SICUREZZA 2

LA SICUREZZA DELL'INFORMAZIONE 4

LA CRITTOGRAFIA 5

I CRIMINI NEL DIGITALE 6

PRINCIPALI TIPI DI ATTACCO 7

BIBLIOGRAFIA 9

IL FATTORE UMANO E Il SOCIAL ENGINEERING

La sicurezza non è solo un problema tecnologico: è una questione legata anche e soprattutto alle persone.
Social engineering è un termine diffuso da Kevin Mitnick, *hacker* divenuto consulente, che indica le attività atte a indurre le persone a compiere azioni o a rivelare informazioni personali in maniera inconsapevole.
Peggiori delle più invadenti minacce informatiche, le minacce basate sull'ingegneria sociale sono le più difficili contro cui proteggersi perché prendono di mira le persone e non solo il sistema informatico.
Il modo più efficace per proteggersi da questi rischi è mantenersi informati: sapere da cosa guardarsi, che cosa evitare e a cosa prestare attenzione.
Il *social engineering* mette insieme una serie di tecniche, non necessariamente informatiche, che inducono la vittima a eseguire azioni che solitamente hanno l'obiettivo di ottenere informazioni e strumenti necessari a compiere attività fraudolente.

Come difendersi dal social engineering.

La contromisura più efficace per ostacolare l'azione del social engineering è aumentare il proprio grado di consapevolezza e discutere delle tecniche e dei più recenti approcci, che magari abbiamo anche subito, con familiari, amici, conoscenti, colleghi, partner e clienti. Se si aumenta la comprensione del fenomeno e la consapevolezza delle conseguenze, siamo agevolati a riconoscerne le tecniche, le caratteristiche della sua azione, evitando così di cadere nelle trappole tese.
Nelle organizzazioni – come ad esempio le aziende – il *social engineering* può essere ostacolato focalizzando gli sforzi su sessioni di *security awareness* (consapevolezza dei rischi e della sicurezza) destinate al personale e in particolare ai dipendenti che trattano informazioni critiche, nonché investendo sugli aspetti di separazione dei ruoli e sulle misure di monitoraggio.

Oggi, soprattutto, si possono ottenere informazioni un tempo difficili da reperire che possono essere usate per entrare nei data base delle aziende.
Con uno smartphone si possono fotografare documenti, disegni, progetti, oppure ci si può connettere alla rete interna, se non ben protetta, inviando al di fuori documenti senza lasciare traccia.
Per prevenire queste minacce non è sufficiente installare sistemi di controllo, come ad esempio un antivirus. Bisogna invece adottare regole e procedure di comportamento e dare vita ad una vera e propria "operazione culturale" sulla gestione dei dati dell'organizzazione.
Per innalzare i livelli di sicurezza, oltre a definire dei buoni comportamenti, è essenziale elevare la conoscenza informatica degli utenti.

L'utilizzo dei computer e degli altri apparecchi aziendali deve essere riservato a scopi professionali e non ad attività private. Questa intuitiva regola di base evita, ad esempio, che l'utilizzo errato di un computer in una rete provochi malfunzionamenti a tutti gli apparecchi presenti nella rete stessa e addirittura bloccare alcune attività con danni difficilmente calcolabili.
Tra gli aspetti comportamentali da prendere in considerazione per la sicurezza nell'uso del digitale e delle tecnologie informatiche, possiamo elencare le seguenti attenzioni:

- Sulla Password - La password è personale e segreta, ma spesso viene data all'amico, al collega, o addirittura all'ospite. Una pratica da evitare.
- Sull'apparecchiatura informatica – Se lasciamo il notebook sulla scrivania e ci allontaniamo, deve essere spento o bisogna configurare il salvaschermo con password, in modo da evitare accessi indesiderati.
- Sui Download – È importante prestare attenzione ai siti da cui si scarica, soprattutto a quelli che offrono download gratuiti. È indispensabile controllare che non si aprano altre finestre, che non ci siano autorizzazioni di qualche tipo già spuntate e approvate.
- Sui supporti esterni – Chiavette USB e hard disk esterni possono contenere programmi infetti. Prima di trasferire dati sul PC, bisogna analizzarne il contenuto con l'antivirus.
- Sul telefono - Attenzione a telefonate in cui vi si chiedono password e utenze: banche o altre aziende non chiedono mai qualcosa di riservato ai propri clienti.
- Sugli allegati nelle email - La mail che rende milionari o ci fa vincitori della lotteria è un elemento di sicuro dubbio, pertanto non inseriamo le credenziali e soprattutto non apriamo gli allegati della mail. Spesso le mail con un collegamento sospetto arrivano dalla persona che conosciamo e della quale ci fidiamo, ma è meglio fermarsi: il nostro amico può aver subìto un attacco che ne ha carpito la rubrica e ora sta inviando email a tutti i suoi contatti. In ogni caso, la miglior politica è non aprire nessun allegato a meno di non sapere già di cosa si tratta.

LA SICUREZZA

Secondo le norme ISO la **sicurezza** è definita come "l'insieme degli sforzi dedicati ad assicurare la protezione dei dati e delle risorse di sistema in termini di **integrità, riservatezza e disponibilità**".
Per **integrità** (**Integrity)** si intende l'insieme delle azioni volte a "prevenire la modifica inopportuna di dati o funzionalità del sistema"
La **riservatezza (Confidentiality)** è stata definita dalla International Organization for Standardization (ISO) in ISO-17799 come "la garanzia che le informazioni siano accessibili solo a chi è autorizzato ad accedervi"
Con **disponibilità** (**Availability)** si intende "il tempo in cui un sistema è disponibile ad operare in uno stato affidabile".

Più in generale per **sicurezza di un sistema informatico si intende** la salvaguardia di questi aspetti fondamentali:

- ❑ affidabilità
- ❑ integrità
- ❑ riservatezza
- ❑ autenticità
- ❑ non ripudio

Si definisce **sicuro** un sistema informatico nel quale le informazioni contenute sono garantite attraverso **sistemi e misure di sicurezza** appositamente predisposti contro il pericolo di violazioni.

Il controllo degli accessi

Il primo aspetto di sicurezza da definire nei sistemi informatici è il controllo degli accessi. Nei sistemi è necessario definire gli utenti abilitati all'accesso, le risorse a cui hanno accesso e in che modalità possono accedervi**. L'accesso** ai sistemi avviene attraverso tre fasi distinte:

- **Identificazione**: *Chi siete? (user id)*
  L'**Identificazione** è una procedura organizzativa e tecnologica attraverso la quale si verifica l'identità dell'utente:
  - l'identità fisica dell'individuo
  - le caratteristiche rispetto al servizio rilasciato (ruolo, stato civile, fedina penale…)

  L'utente che vuole accedere a un sistema, sia esso un computer, un server, un bancomat, deve quindi "rispondere" a questa domanda **di controllo/identificazione per l'accesso.** Nella maggior parte dei casi la risposta è il login, username, user-id o la chiave pubblica (Questa informazione può infatti essere pubblica, non coperta cioè da nessun vincolo di segretezza)

- **Autenticazione**: *Come potete dimostrare la vostra identità? (password)*
  Una volta stabilità l'identità, il sistema deve essere sicuro che l'utente sia quello che dice di essere.
  La risposta è la *password*, legata allo username con cui ci si è identificati, o il codice PIN, ma anche una chiave privata, la propria impronta digitale o l'iride dell'occhio.
  Questa informazione deve essere assolutamente tenuta **segreta** e conservata con la massima accuratezza.

- **Autorizzazione**: *Cosa siete autorizzati a fare? (permessi)*
  Identificato, autenticato e abilitato l'utente, si tratta di stabilire a quali risorse e informazioni può accedere.
  Il sistema è in grado di stabilire quali operazioni consentire e quali vietare attraverso alcuni parametri:

  - **Livello di funzionalità** (es. amministratore, super utente, utente)
  - **Limitazioni di accesso alle risorse** (accesso ai programmi, ad archivi e a cartelle di archiviazione…)

  Normalmente le autorizzazioni sono attribuite a livello di singolo utente e/o di gruppi di utenti per facilitare le operazioni di gestione della sicurezza.

Password: limiti e caratteristiche

L'autenticazione con password viene definita "debole" perché:

- La password ha generalmente una lunghezza limitata
- La password può essere scoperta facilmente
- La password viaggia spesso in chiaro sulla rete di comunicazione

Per questo motivo ci sono algoritmi (detti di *hash)* che consentono di non far viaggiare in chiaro i dati. Spesso, in relazione all'importanza del servizio a cui si accede, si procede all'autenticazione con riconoscimento biometrico:

- Riconoscimento delle impronte digitali (fingermarks)
- Scansione della retina (retina scan)

La "*strong authentication*"

I protocolli di autenticazione sono quelle procedure attraverso le quali è possibile verificare che un utente sia effettivamente chi dice di essere.
L'autenticazione può essere fatta sostanzialmente in tre diverse modalità che prevedono l'utilizzo di:

1. ***Something You Know*** (Qualche cosa che si sa): questa modalità è quella realizzata mediante l'utilizzo della password
2. ***Something You Have*** (Qualche cosa che si ha): per esempio una chiave fisica, un tesserino magnetico o un codice variabile tipo Secur-Id che si può portare con sé

3. ***Something You Are*** (Qualche cosa che si è) ad esempio un parametro biometrico come l'impronta digitale o l'immagine dell'iride

Se si utilizzano almeno due di queste modalità si parla di **autenticazione forte**
Nelle reti e nei sistemi distribuiti si adottano le tecnologie di cui al punto 1. Nei sistemi di pagamento si adottano sistemi misti basati sui punti 1 e 2.

Biometria e Password.

Biometria è la nuova parola chiave per le procedure di sicurezza. Ma cosa intendiamo per sistemi biometrici di controllo e sicurezza?
Sono sistemi che permettono l'identificazione di una persona sulla base di una o più caratteristiche biologiche e/o comportamentali confrontate con dati, acquisiti precedentemente, e memorizzati tramite algoritmi e sensori.
Dopo impronte digitali, utilizzate per l'accesso personale di alcuni smartphone, oggi siamo in presenza addirittura di grilletti che si applicano alle armi da fuoco e funzionano solo se l'arma è impugnata dal proprietario.
In un futuro molto prossimo saranno commercializzati dispositivi mobili con scanner per lettura dei movimenti degli occhi, movimenti che sono unici per ciascuno di noi.
In quel momento basterà un selfie per autenticare la carta di credito, il battito del polso potrebbe aprire la portiera dell'auto e l'accesso al computer potrà avvenire con il movimento degli occhi o avvieremo il motore dell'auto solo con lo sguardo.
La biometria tende a soppiantare l'uso delle password perché si basa sul "chi siamo".

Nel 2015, secondo il Biometric Research Group, almeno già 650 milioni di persone nel mondo hanno usato un sistema biometrico su dispositivi mobili e da qui al 2020 questo numero potrebbe crescere del 20 per cento. Un segnale inequivocabile che occhi, volto, cuore e dita stiano lentamente ma inesorabilmente diventando un metodo alternativo alle parole chiave ormai non più sicure.
Niente più problemi di sicurezza quindi? No, non esiste una biometria non falsificabile, se ci rubano una password infatti possiamo sostituirla, ma se ci rubano l'impronta digitale?

LA SICUREZZA DELL'INFORMAZIONE

La sicurezza si applica anche ai dati gestiti nei sistemi informatici e digitali. Applicare sicurezza ai dati, e quindi alle informazioni, significa rispettare queste proprietà:

Affidabilità
È la proprietà che devono possedere i dati per essere sempre accessibili o disponibili agli utenti autorizzati.
Esempi di violazione di questa proprietà sono:

- mancanza di fornitura elettrica,
- rottura di un componente hardware.

Integrità
È la protezione dei dati realizzata in modo da evitare la loro corruzione. In particolare, nella trasmissione, i dati devono arrivare così come trasmessi, mentre nella memorizzazione, i dati devono coincidere in ogni istante con quelli memorizzati originariamente. L'integrità riguarda la protezione da modifiche non autorizzate, come ad esempio la cancellazione non autorizzata e la modifica non autorizzata.

Riservatezza
È la protezione dei dati realizzata in modo che essi siano accessibili in lettura solo dai legittimi destinatari. Si dice che la riservatezza riguarda la protezione da letture non autorizzate.
Esempi di violazione sono:

- intercettazione di dati durante la trasmissione,
- accesso non autorizzato ai dati su un server.

Autenticità
È la protezione sulla certezza della sorgente, della destinazione e del contenuto del messaggio.
Un esempio di violazione è:

- la spedizione di una e-mail da parte di un pirata informatico che si maschera facendo credere che il mittente dell'e-mail sia una persona conosciuta al destinatario.

Non ripudio
Consente di associare il dato a colui che lo ha sottoscritto. È la protezione sulla certezza che chi trasmette (non ripudio del mittente) e chi riceve (non ripudio del destinatario) non possano negare di aver inviato e ricevuto i dati.
Esempi di non ripudio dalla vita di tutti i giorni in situazioni simili a quelle informatiche sono:

- una raccomandata con ricevuta di ritorno garantisce il non ripudio da parte del destinatario, in quanto questi deve firmare di persona la ricevuta di ritorno (è garanzia pertanto anche la sua autenticità),
- l'autenticazione della firma da parte di un pubblico ufficiale garantisce, invece, il non ripudio del mittente (oltre alla sua autenticità),

Esempi di violazione nella comunicazione informatica sono:

- carta intestata falsa,
- firma falsa,
- falsa e-mail.

LA CRITTOGRAFIA

La crittografia viene applicata nel contesto della sicurezza e dello scambio di dati.
Dal greco *kryptos*, nascosto, e *graphein*, scrivere: è il processo che trasforma il "testo puro" in "testo cifrato", la Crittografia richiede un **algoritmo** e una **chiave.**
Per la sicurezza non è importante l'algoritmo (può essere pubblico) ma la chiave utilizzata, che deve rimanere segreta.
Lo scopo è coprire i punti chiave della sicurezza quali:

- **Integrità**
- **Riservatezza**, **Confidenzialità, Privacy**
- **Autenticazione**
- **Non ripudio**

La crittografia può assumere due forme:

- **La crittografia simmetrica (chiave privata):** algoritmo con chiave unica segreta per cifrare e decifrare il testo.
  La sicurezza è nella bontà della chiave.
  Per operazioni di codifica e decodifica si utilizza la stessa chiave. Sono detti algoritmi simmetrici e la segretezza è legata alla segretezza (e complessità) della chiave. Viene resa sicura utilizzando chiavi monouso generate in modo casuale

- **La crittografia asimmetrica (chiave pubblica):** algoritmo che utilizza due chiavi differenti per cifrare e decifrare il testo.
  In questi algoritmi non esistono problemi nella gestione della chiave segreta perché non deve essere distribuita, ma utilizzata solo da chi l'ha generata.
  Se le informazioni sono criptate con chiave privata, solo la chiave pubblica è in grado di decriptarle
  Se le informazioni sono criptate con chiave pubblica, solo la chiave privata è in grado di decriptarle
  La chiave privata, segreta, non deve essere diffusa e rimane di proprietà della persona che la crea, la seconda chiave pubblica deve essere resa pubblica.
  Con un algoritmo non reversibile (*one-way*) ciò che viene cifrato utilizzando una delle due chiavi può essere decifrato solo con l'altra.
  La generazione e l'assegnazione delle chiavi pubbliche viene effettuato da una CA (*Certification Authority*)
  L'insieme degli standard e delle tecnologie utilizzate si chiama di PKI (*Public Key Infrastructure*)

La **crittografia asimmetrica** può essere anche usata per provare l'identità di tutte le parti che hanno partecipato ad una transazione (cioè lo scambio di un messaggio tra due parti) anche successivamente al momento dell'effettuazione, si usa cioè per avere la certezza dell'autore del messaggio (**paternità**).
Il firmatario di un documento trasmesso non può negare di averlo inviato, né può il ricevente negare di averlo ricevuto, più semplicemente, con **non ripudio** si intende che l'informazione non può essere disconosciuta, come una firma a mano davanti a testimoni su un documento.

La Firma Digitale

La **firma digitale** è un metodo di identificazione informatica basato su varie tecnologie, tra cui la crittografia a chiave pubblica.

La firma di un documento digitale soddisfa tre esigenze:

- che il destinatario possa verificare l'identità del mittente (**autenticazione**);
- che il mittente non possa disconoscere un documento da lui firmato (**non ripudio**);
- che il destinatario non possa inventarsi o modificare un documento firmato da qualcun altro (**integrità**).

Il sistema per la creazione e la verifica di firme digitali sfrutta le caratteristiche della crittografia asimmetrica.
Un sistema crittografico garantisce la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso della "chiave" per interpretarli. Nei sistemi crittografici a chiave pubblica, detti anche a chiave asimmetrica, ogni utente ha una coppia di chiavi: una chiave privata, da non svelare a nessuno, con cui può decifrare i messaggi che gli vengono inviati e firmare i messaggi che invia, e una chiave pubblica, che altri utenti utilizzano per cifrare i messaggi da inviargli e per decifrare la sua firma e stabilirne quindi l'autenticità.
Perché il sistema sia sicuro, è necessario che solo l'utente e nessun altro abbia accesso alla chiave privata. Il modo più semplice per ottenere questo è far sì che l'unica copia della chiave sia "in mano" all'utente (il quale deve impedirne l'accesso a terzi).
Lo scenario in cui un mittente vuole spedire un messaggio a un destinatario in modalità sicura è il seguente: il mittente utilizza *la chiave pubblica del destinatario* per la cifratura del messaggio da spedire, quindi spedisce il messaggio cifrato al destinatario; il destinatario riceve il messaggio cifrato e adopera la propria chiave privata per ottenere il messaggio "in chiaro".
Grazie alla proprietà delle due chiavi un sistema di crittografia asimmetrica di questo tipo è adatto anche per ottenere dei documenti firmati, ma in modalità inversa rispetto a quella appena descritta cioè con la chiave privata a cifrare e quella pubblica a decifrare. Infatti, la chiave pubblica di un utente è la sola in grado di poter decifrare correttamente i documenti cifrati con la chiave privata di quell'utente.
La titolarità della firma elettronica qualificata è garantita dai "certificatori", soggetti con particolari requisiti di onorabilità che garantiscono affidabilità organizzativa, tecnica e finanziaria. I certificatori hanno il compito di tenere i registri delle chiavi pubbliche, al fine di verificare la titolarità del firmatario di un documento elettronico.
I certificatori, inoltre, possono essere accreditati presso l'Agenzia per l'Italia digitale (AgID) e in tal caso vengono chiamati certificatori accreditati.
L'acquisizione della coppia di chiavi (chiave privata, inserita nel dispositivo di firma sicuro, e chiave pubblica, inserita nel certificato) è a pagamento, attraverso la sottoscrizione di un contratto con il certificatore accreditato. La coppia di chiavi ha una scadenza temporale, al momento 3 anni. Il rilascio avviene con l'identificazione certa del firmatario da parte del certificatore perché sia certa l'associazione che il certificato effettua tra chiave pubblica e dati anagrafici del titolare della firma.

I CRIMINI NEL DIGITALE

Qualsiasi sistema digitale connesso alla rete è potenzialmente vulnerabile ad un attacco.
Un «attacco» è lo sfruttamento di una vulnerabilità per scopi non conosciuti da chi utilizza il sistema e generalmente pregiudizievoli.
Fra i principali "crimini digitale" si possono individuare:

- pubblicazione su internet o altri canali informatici di contenuti di attività illegali (pedofilia, xenofobia e incitamento alla violenza politica e/o razziale)
- accesso non autorizzato a sistemi riservati o danni connessi all'intasamento delle risorse con indisponibilità del servizio (**denial of service**)

- diffusione di virus, o il cosiddetto procurato allarme (**hoax**), es. la diffusione di messaggi che inducono i più sprovveduti a cancellare alcuni file di sistema sconosciuti ma non infetti;
- truffe on line

Gli attacchi crescono esponenzialmente sia di numero che gravità e il denominatore comune è la compromissione di elevatissime quantità di dati sensibili.

Gli attacchi sono spesso lanciati automaticamente a partire da sistemi infettati all'insaputa dei loro utilizzatori, o in altri casi frutto di azioni da parte di pirati informatici. Nel mondo della pirateria digitale sono definibili due figure: hacker e cracker.

Hacker
Un *hacker* è una persona che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte.
Esiste un luogo comune, usato soprattutto dai mass media (a partire dagli anni '80), per cui il termine *hacker* viene associato ai criminali informatici (la cui definizione corretta è, però, cracker).

Cracker

È colui che si ingegna per eludere blocchi imposti da qualsiasi software in genere.
I *cracker* possono essere spinti da varie motivazioni, dal guadagno economico (tipicamente coinvolti in operazioni di spionaggio industriale o in frodi) all'approvazione all'interno di un gruppo di *cracker*.
Il termine *cracker* viene spesso confuso con quello di *hacker*, il cui significato, come accennavamo, è tuttavia notevolmente diverso. Alcune tecniche sono simili, ma l'intenzione dell'*hacker* è generalmente l'esplorazione, il divertimento, l'apprendimento, senza creare reali danni.
È indispensabile quindi conoscere i principali tipi di attacchi per poter attuare delle azioni di prevenzione.

PRINCIPALI TIPI DI ATTACCO

Backdoor Trojans
È un programma che consente di prendere il controllo del computer di un utente. **Backdoor** significa porta posteriore, e i Trojan Horse (**Cavallo di Troia**) sono un tipo particolare di *backdoor* che una volta "entrato" nel sistema si presenta come un programma innocuo. Rimane in "ascolto" e può accettare comandi per effettuare azioni nocive. I trojan ono molto diffusi in quanto possono essere facilmente inviati tramite posta elettronica come allegati. Oltre che dalla posta possono essere veicolati anche da semplici pagine web apparentemente innocue.
Bluesnarfing
Consiste nella sottrazione dei dati presenti su un telefono cellulare provvisto di tecnologia Bluetooth.
Browser hijacking
Il "dirottamento del browser" consiste nella modifica involontaria della pagina iniziale e le pagine di ricerca del programma di navigazione.
Denial-of-service (Attacco DoS)
Un attacco DoS (Denial-of-service, letteralmente "negazione del servizio") impedisce agli utenti di accedere a un computer o sito Internet.
Internet worm
Sono programmi che si diffondono attraverso le connessioni Internet. Si caratterizza per la capacità di replicarsi continuamente.
"Phishing"
Consiste nell'uso di e-mail e di falsi siti Web per indurre gli utenti con l'inganno a fornire informazioni confidenziali o personali. Viene inviata una e-mail in cui si chiede di installare un software allegato (un falso "aggiornamento di sicurezza" di Windows) o di leggere un documento o visitare un certo sito (*pericoloso*).
L'allegato o il sito contengono software infetti o rubano dati personali
"Rootkit"
È un software in grado di nascondere i programmi o i processi installati sul computer. Viene solitamente utilizzato per sottrarre dati o per eseguire operazioni illecite.
Spyware
È un software che permette a società commerciali e cracker di raccogliere informazioni a insaputa dell'utente.
Virus

È un piccolo programma o un "pezzo" di codice che viene inserito all'interno di altri programmi e viene attivato all'esecuzione del programma e al verificarsi di eventi particolari può effettuare un attacco di tipo distruttivo. È in grado di propagarsi infettando altri programmi (anche via rete).

Consigli di protezione

Spesso, come abbiamo visto, il migliore antivirus possiamo essere noi stessi, e riprendendo anche parte del discorso iniziale sul *Social Engineering*, possiamo praticare e scegliere una serie di attenzioni e accorgimenti che rendono ancora più efficace la protezione, quali:

- ✓ **Usate un software antivirus**. È bene prevedere un sistema con l'aggiornamento automatico.
- ✓ **Usate un firewall sui computer collegati a Internet**.
- ✓ **Aggiornate il sistema con le patch di sicurezza**. Le patch correggono le vulnerabilità del sistema.
- ✓ **Effettuate backup regolari dei programmi e dei dati**.

Evitare il phishing

- Non rispondete mai a messaggi che chiedono informazioni finanziarie e personali.
- Verificate che la connessione sia protetta. Se il sito che visitate si trova su un server protetto, il collegamento deve iniziare con https://. Inoltre verificate che ci sia l'icona del lucchetto nella barra di stato del browser.
- Attenti a gestire e-mail e dati personali. Non rivelate a nessuno e non riscrivete il codice PIN o la password. Non aprite messaggi di spam e non rispondete. Il rischio è di confermare che l'indirizzo di posta è valido e, in seguito, potreste essere vittima di truffe on-line.

Navigare sicuri

- **Non cliccate sulle finestre popup**. Specialmente se avvertono della presenza di virus sul computer e offrono soluzioni, non selezionate il link e non autorizzate nessun download. Potreste scaricare e installare software dannosi.
- **Non cliccate sui link presenti all'interno dei messaggi di posta indesiderata**. Possono indirizzarvi su un sito fittizio, utilizzato per avere informazioni personali, come dettagli bancari e password.
- **Configurate il browser Internet per garantire la massima sicurezza** disabilitando i controlli Java o Active X, o chiedendo di essere avvisati prima dell'esecuzione.

Scegliere la password

Le password permettono di proteggersi da frodi e sottrazioni di informazioni riservate, ma poche persone scelgono password davvero sicure.

Scegliete una password lunga. Più è lunga, più è difficile da decifrare o indovinare utilizzando tutte le combinazioni (usate almeno otto caratteri).

Usate caratteri diversi, tra cui numeri, segni di punteggiatura, lettere maiuscole e minuscole.

Non usate parole contenute nei dizionari. Gli hacker possono sferrare un *dictionary attack* provando a inserire, in automatico, tutte le parole contenute nel dizionario.

Non inserite informazioni personali. Altre persone possono conoscere la vostra data di nascita, il nome del partner o del bambino, il numero di telefono e potrebbero così indovinare la password.

Non scegliete una password uguale al vostro username o al numero di conto.

Scegliete una password difficile da identificare durante la digitazione (non usare caratteri ripetuti o tasti vicini sulla tastiera).

Valutate l'uso di una frase chiave, ossia un insieme di parole o di stringhe alfanumeriche. Abbinamenti insoliti sono difficili da decifrare.

Memorizzate le vostre password invece di scriverle. Scegliete una combinazione significativa per voi per facilitarne la memorizzazione.

Non salvate le password sul computer o su dispositivi online. Qualcuno potrebbe accedere al vostro computer e trovare le password.

Non tenete le password vicino al computer o in un posto facilmente accessibile.

Utilizzate password diverse per ogni account.

Non rivelate a nessuno le password. Se un modulo via email che vi richiede di confermare le vostre password, evitate di compilarlo anche se la fonte sembra attendibile (vedi Phishing).

Non inserite le vostre password se usate computer di pubblica utenza, come quelli disponibili negli hotel o negli internet point.

Cambiate le vostre password con regolarità, soprattutto se corte o semplici da indovinare.

LE SFIDE DELLE NUOVE OPPORTUNITA'

L'individuazione delle opportune misure di sicurezza è una continua rincorsa in diverse direzioni. Da una parte gli hacker e i cracker escogitano sempre nuove e più raffinate modalità di intrusione e di danneggiamenti. Dall'altra l'evoluzione delle versioni dei sistemi operativi e di rete offre spesso nuove brecce nei sistemi di sicurezza che gli hacker possono riuscire ad individuare e ad avvalersene per i loro intenti criminali.

Ma anche l'evoluzione dei comportamenti e delle organizzazioni può creare vulnerabilità se non ben gestite e protette.

E' questo il caso, ad esempio, della soluzione organizzativa di consentire ai dipendenti delle aziende di utilizzare i propri dispositivi mobili anche per accedere ed utilizzare, dal proprio posto di lavoro o ovunque, le applicazioni aziendali e quindi intervenire sui dati aziendali.

Questa politica che ha preso il nome di **BYOD** (acronimo di **Bring Your Own Device**) è gradita ai lavoratori che utilizzano per uso personale e sul lavoro un unico strumento, quello che hanno scelto loro stessi, che apprezzano e conoscono quindi molto bene.

Il vantaggio è tanto più evidente quando altrimenti lavoratore e azienda impiegassero soluzioni diverse, per esempio una soluzione Open Source a casa e prodotti proprietari in azienda.

La politica aziendale del BYOD comporta però per l'azienda accresciuti rischi per la sicurezza e conseguentemente costi per proteggersi da tutte le tipologie di dispositivi e specialmente dalle app che ognuno ha scelto di installare per l'uso personale, protezioni che devono agire sui diversi dispositivi, sotto il controllo del proprietario.

BIBLIOGRAFIA

TITOLO	AUTORE	EDIZIONI	ANNO
L'arte dell'inganno	Kevin D. Mitnik	Feltrinelli	2005
Piccolo Manuale Della Sicurezza	Riccardo Meggiato	Apogeo	2011
Hacker 7.0	Stuart McClure, George Kurtz, Joel Scambray	Apogeo	2013
L'arte dell'hacking	Kevin D. Mitnik William L. Simon	Feltrinelli	2014
Il Rumore dell'Hacking – I percorsi silenziosi dell'informazione	Michal Zalewski	Apogeo	2005
Privacy e sicurezza digitale	Daniel G. Bachrach, Eric J. Rzeszut	Tecniche Nuove	2015