CYBERSECURITY: CONOSCERE PER DIFENDERSI

IL RUOLO FONDAMENTALE DELL'INDIVIDUO NELLA TUTELA DEI DATI E DELLA REPUTAZIONE ONLINE

A cura di intuity, azienda specializzata
in servizi per la Cybersecurity

skilla
il metodo di
amicucci formazione

"I computer sono incredibilmente veloci, accurati e stupidi. Gli uomini sono incredibilmente lenti, inaccurati e intelligenti. L'insieme dei due costituisce una forza incalcolabile."

Albert Einstein

INTRODUZIONE

La nostra vita quotidiana è sempre più caratterizzata dalla presenza di strumenti tecnologici. A casa, nel tempo libero, a lavoro.
Molti di questi sono interconnessi o comunicano con Internet. Significa cioè che "dialogano" tra di loro o con altri elementi a noi più o meno sconosciuti.

Tutto questo è molto utile: possiamo condividere foto, le nostre performance sportive, navigare in Internet dalla televisione di casa, scambiarci documenti di lavoro mentre siamo in treno, ordinare regali seduti sul nostro divano, attingendo da cataloghi virtualmente infiniti.

Se per noi ciò costituisce un miglioramento della vita quotidiana, per qualcun altro diventa un'interessante opportunità di business. Tra questi c'è chi lo fa in modo fraudolento, cercando di accedere ai dati registrati nei nostri dispositivi, ottenere pagamenti non dovuti, indurci a compiere azioni contro il nostro interesse o fare qualcosa usando la nostra identità.
Ecco perché occorre essere sempre vigili e un tantino diffidenti ogni qualvolta usiamo uno strumento tecnologico o siamo on-line.
Basti pensare che secondo il rapporto dell'Associazione Italiana per la sicurezza informatica non sono mai stati registrati tanti attacchi informatici come nel 2016: phishing a +1166%, cyber warfare a +117%. Tra i settori più presi di mira la sanità (+102%), la GDO (+70%) e il banking-finance (+64%). [1]

[1] *Fonte: https://www.corrierecomunicazioni.it/digital-economy/clusit-2016-annus-horribilis-per-il-cybercrime/*

I CYBERCRIMINALI

Ma chi sono questi "cattivi della Rete"? Quale interesse hanno nel realizzare delle frodi informatiche?

Qualcuno li chiama hacker, ma non è la definizione corretta. L'**hacker** è normalmente mosso da finalità di ricerca ed approfondimento: usa metodi non sempre legali, ma per scopi positivi. I **"pirati" della Rete** sono invece dei veri e propri delinquenti che agiscono per fini di lucro.

Questi possono essere:

- ragazzi più o meno esperti nell'uso del PC che vogliono guadagnare qualche soldo;
- piccole organizzazioni criminali che rivendono dati aziendali o usano la tecnica del riscatto;
- grandi organizzazioni malavitose che vedono nella frode on-line un business dal valore di centinaia di miliardi di euro.

Tutto questo è facilitato dall'anonimato che la Rete riesce a garantire e che molto spesso fa in modo che queste attività illegali rimangano impunite.
Ognuno di noi può essere una vittima, sia come privato cittadino, sia come possibile punto di accesso per raggiungere i dati dell'azienda per cui lavoriamo.

CURIOSITÁ

Sapevi che il termine hacker in origine identificava un gruppo di appassionati di modellismo?
Tutto è nato al MIT, Massachusets Institute of Technology di Cambridge, dove un gruppo di studenti si dedicava a smontare e riassemblare trenini e componenti elettromeccanici.

Il termine "Hacker" infatti ha un'accezione positiva, di colui che ha desiderio di capire come funzionano le cose per modificarle a suo piacimento.

Col tempo il significato è mutato drasticamente, almeno nella percezione comune ed identifica ora il cosidetto "Pirata informatico".

Per approfondire:
https://en.wikipedia.org/wiki/Tech_Model_Railroad_Club

e per consocere la storia dell'hacking in Italia:
https://it.wikipedia.org/wiki/Spaghetti_hacker

QUALI TECNICHE USANO GLI HACKER?

Tipicamente chi attacca ha due scelte:
1. Cercare delle vulnerabilità in un sistema informatico
2. Sfruttare le vulnerabilità dell'essere umano

Vediamo cosa significa.

Attacco ad un sistema informatico
Molti degli strumenti che usiamo quotidianamente sono pilotati da uno o più programmi, definiti software: ad esempio il sistema operativo di un computer è un **software** (Windows, Linux, MacOS, Android, iOS), ma anche tutte le applicazioni o APP che usiamo sono software (Word, Acrobat Reader, ecc.).

Il software è un prodotto dell'uomo, il programmatore, il quale, per quanto bravo e attento sia, può commettere degli errori: quest'ultimi prendono il nome di "**bug**" o "**vulnerabilità**".

Queste vulnerabilità possono consentire, a chi le sa sfruttare, di accedere al sistema, comandarlo a suo piacimento o fargli compiere delle azioni non previste.

Quindi un bravo hacker, riesce a rilevare le vulnerabilità di un sistema e trovare il modo di usarle per raggiungere i suoi scopi.
Molto spesso però siamo noi gli "artefici" di queste vulnerabilità: immagina di aver comprato un nuovo disco di rete da installare in casa per conservare foto e documenti, al quale puoi accedere tramite smartphone quando ti trovi in giro. Se in fase di installazione non hai modificato la password di accesso lasciando quella di fabbrica, chiunque connesso ad Internet lo raggiunga potrebbe facilmente entrare ed accedere alle tue preziose informazioni.

CURIOSITÁ

Pensi che le vulnerabilità presenti nei vari software siano poche? Prova a guardare questo sito: https://www.exploit-db.com/

Verifica ora se ne esiste qualcuna anche su strumenti a te familiari.

Attacco all'essere umano: Social Engineering
Cosa c'entra l'essere umano parlando di hacking? C'entra molto di più di quanto si possa immaginare, anzi: è molto più diffuso ed efficace far leva sul "fattore umano" piuttosto che andare alla ricerca delle vulnerabilità.

L'hacking alle persone prende il nome di **Social Engineering**: si tratta di indurre qualcuno a fare qualcosa tramite l'inganno o la persuasione, facendo leva sulle "vulnerabilità" tipiche dell'essere umano:

- curiosità
- fretta
- emozione
- paura

Nel mondo della cybersecurity il Social Engineering è diventato il primo metodo con cui realizzare un attacco informatico. Tre sono le tecniche maggiormente utilizzate:

- Impersonification
- Baiting
- Phishing

Impersonification significa, fare finta di essere qualcun altro.

Immagina ad esempio un hacker che vuole ottenere i file di un progetto importante di un'azienda. Identifica le persone legate al progetto usando Linkedin e studia le loro abitudini tramite Facebook. Scopre quindi che il capo del progetto X è in vacanza per una settimana. L'hacker chiama allora il reparto di sviluppo fingendosi l'assistente del capo progetto incaricato di recuperare alcuni documenti tecnici per un potenziale cliente. Se la persona contattata non è attenta può succedere che condivida questi file senza porsi molte domande.

CURIOSITÁ

Pensi che questa sia una storia inventata o irreale?

Ascolta questo racconto di Kevin Mitnick, uno degli hacker più conosciuti al mondo, tratto dal documentario "Lo and Behold":
https://www.youtube.com/watch?v=LROOnX4R_jE

Baiting è un'altra tecnica molto efficace che consiste nel lasciare delle "esche", come ad esempio delle chiavette USB contenenti un virus, in prossimità o all'interno di un'azienda.

Immagina, se nel parcheggio della tua azienda trovassi una chiavetta USB, magari con un'etitchetta che riporta "Prospetto stipendi dirigenti e quadri"... La tentazione di vedere il contenuto della chiavetta sarebbe fortissima!

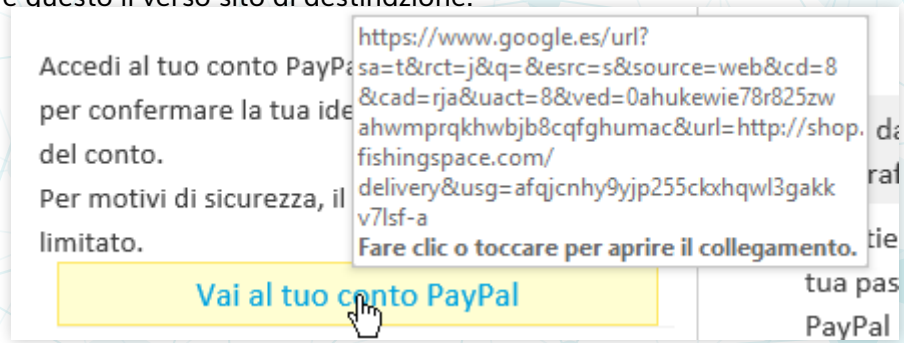
Il **phishing** è sicuramente un termine più noto, che deriva dal termine "pescare": anche in questo caso si usano delle "esche" ma si tratta di e-mail. Il vantaggio di quest'ultima è che può essere inviata a centinaia di persone contemporaneamente senza neppure spostarsi dalla propria postazione di lavoro. Questo è uno dei motivi per cui il phishing è diventato così popolare come metodo di attacco.
Come funziona? L'hacker invia alla nostra casella di posta personale o aziendale un messaggio che suscita il nostro interesse e siamo indotti ad assecondare qualunque richiesta:

- la propria banca, Facebook, LinkedIn, ecc. che ci invitano a modificare la password entro poche ore;
- un servizio di e-commerce che ci avvisa che è stato effettuato un ordine a nostro nome;
- un operatore che ci invia una fattura;
- l'invito a vedere un video o a sottoscrivere una petizione.

Immagina ad esempio di ricevere un'e-mail che ti invita a visionare una favolosa offerta: il nuovissimo SMARTPHONE XYZ al 50% di sconto. Al click sul link che rimanda al sito, un virus potrebbe essere installato nel tuo PC. Il phishing è un metodo di attacco molto insidioso poichè sono molti i modi per nascondere la propria identità e assumerne una apparentemente sicura. Pensa ad esempio di lavorare per l'azienda Axme e di avere come indirizzo di posta elettronica *mario.rossi@axme.it*: un hacker potrebbe registrare un nuovo dominio (ad esempio *supporto-axme. it*) e inviare una e-mail ad un cliente o collega, usando come indirizzo *mario.rossi@supporto-axme.it*.

Le forme di attacco sono quindi le più disparate e la nostra attenzione deve essere massima. Pensiamo sempre: chi mi sta inviando questa e-mail? Perché?

- Mi chiede di modificare una password? Invece di cliccare sul link nell'e-mail, posso andare direttamente sul sito.
- Non fidiamoci del link riportato nel testo del messaggio. Andiamoci sopra con il mouse senza cliccare e guardiamo cosa appare nel pop-up: è questo il verso sito di destinazione.



- Il mittente è veramente chi dice di essere? Guardiamo con attenzione l'indirizzo di provenienza, potremmo notare che invece di Facebook si tratta di Fakebook!
- repaly.com non è PayPal

PayPal <donot@repaly.com>

- Se la richiesta sembra arrivare dalla nostra banca, pensiamoci due volte prima di fare qualsiasi azione.

Quando la vittima di questi attacchi è una persona particolarmente interessante (magari perché dipendente di una grande multinazionale), il cybercriminale può fare ricerche sul suo conto, sui suoi gusti ed abitudini, sulle sue conoscenze, ecc. allo scopo di preparare una e-mail di phisghing estremamente credibile. In questo caso si parla di **whaling**: la pesca alla balena.

VIRUS E MALWARE

L'installazione di un **virus** nei nostri PC è uno dei principali mezzi utilizzati dagli hacker allo scopo di rubare dati, cancellare file, cifrarli per poi chiedere un riscatto per riaverli indietro (ransomware). Esistono anche virus in grado di registrare tutto ciò che facciamo con il nostro computer o addirittura di accedere da remoto e prendere il controllo del sistema.

Il phishing o i siti web compromessi rappresentano spesso un mezzo per riuscire ad installare un virus in un computer.
È bene ricordare che i virus si possono diffondere ad altri computer vicini, in particolare in azienda, dove tutti i pc condividono la stessa rete di comunicazione.

Il nostro livello di attenzione deve essere sempre elevato tenendo in considerazione che sempre più spesso i virus riescono ad eludere i controlli tecnologici, come l'Antivirus, e l'unica difesa che ci rimane è la nostra capacità di riconoscere la minaccia.

- Verifica di avere un buon Antivirus installato nel PC e controlla gli aggiornamenti.
- Se navigando in un sito web ti viene chiesto di installare qualcosa, aspetta e verifica attentamente. Se hai dei dubbi chiedi a qualcuno che ne sa più di te.
- Attenzione alle e-mail! Non aprire gli allegati con troppa leggerezza, è necessario essere estremamente cauti.
- Non inserire nel tuo PC chiavette USB delle quali non conosci l'origine.
- Se percepisci qualcosa di strano utilizzando il PC, segnalalo immediatamente.

FURTO D'IDENTITÁ

L'**identità digitale** è molto complessa ed è rappresentata dall'insieme degli account (username e password) con i quali accediamo ai servizi on-line. Ognuno di questi ci identifica in un particolare contesto: i Social Network, un sito di e-commerce o la banca on-line. Se qualcuno dovesse impossessarsi di tali informazioni potrebbe assumere la nostra identità in quello specifico contesto.

Immaginiamo cosa potrebbe fare un cybercriminale che riesce ad entrare nel nostro account Social: potrebbe "postare" a nostro nome qualunque cosa. Ancora peggio se dovesse accedere al nostro sito di e-commerce preferito, dove magari abbiamo registrato i dettagli della nostra carta di credito.

Per rubare l'identità digitale spesso vengono usate e-mail di "phishing" allo scopo di indurci con l'inganno ad inserire le nostre credenziali in un sito falso, magari facendoci credere che la password sta per scadere o che a causa di un problema dobbiamo riconfermarla.

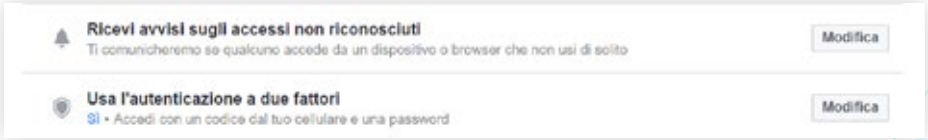
Dobbiamo quindi essere diffidenti ogni qualvolta riceviamo via e-mail o SMS una richiesta di questo tipo: non usare il link che ci viene inviato, ma andare direttamente sul sito, cercando se ci sono avvisi a riguardo o fare l'operazione indicata nel messaggio direttamente dal sito ufficiale.

I principali Social Network, siti di banking on-line e di e-commerce consentono di attivare l'**autenticazione sicura**, che spesso prevede l'invio di un codice sul proprio Smartphone per confermare l'accesso.

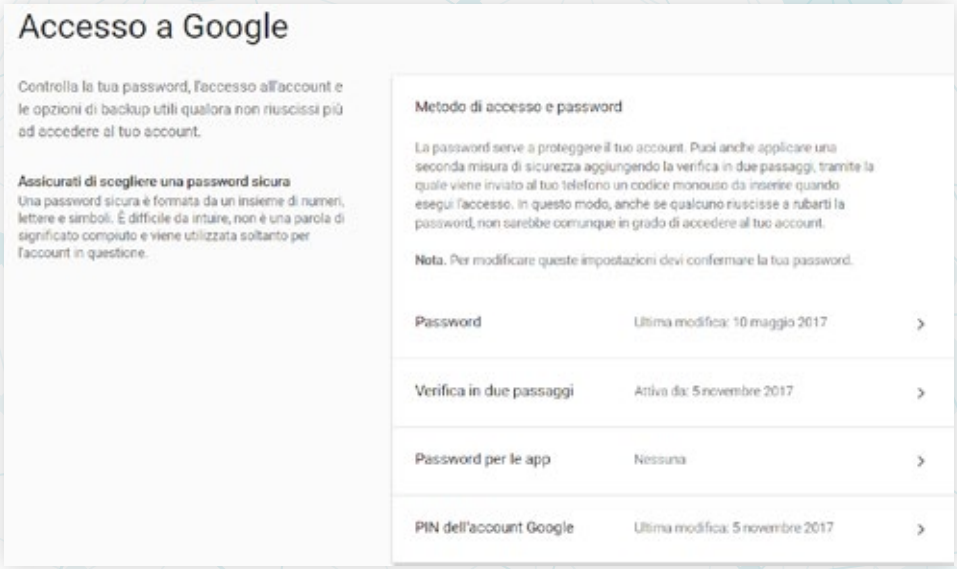
Cerchiamo sempre tra le impostazioni del sito questa opzione e attiviamola: uno sforzo minimo in grado proteggerci da uno dei principali pericoli della rete!

Vediamo alcuni esempi:

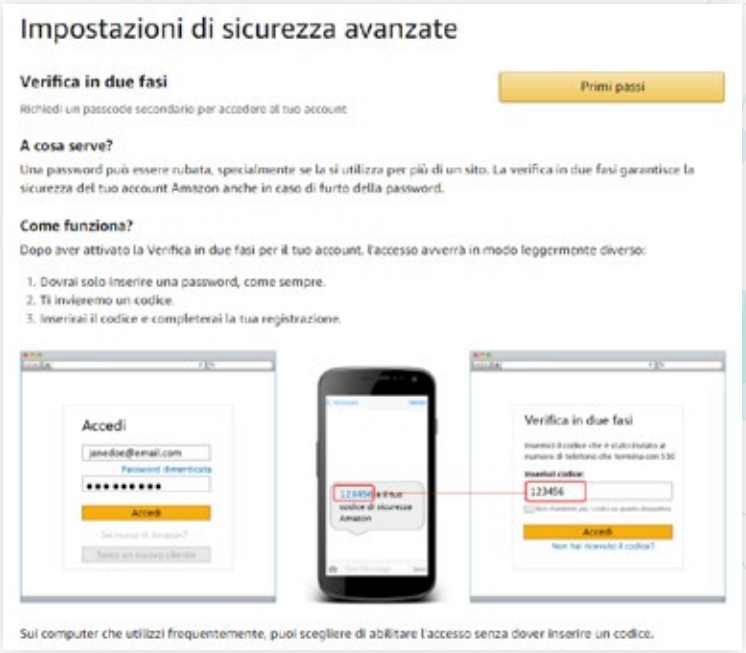
Facebook:



Google:



Amazon:



NAVIGARE IN SICUREZZA

Internet ed i siti web, sono oramai parte integrante della nostra vita: navighiamo per divertimento, per lavoro, per studio, per approfondimento. Qualunque siano i nostri interessi, il Web rappresenta una fonte inesauribile di informazioni.

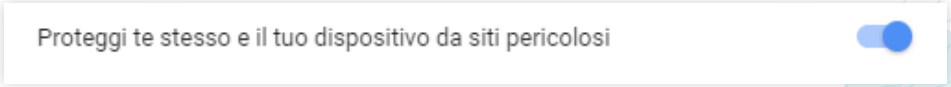
Allo stesso tempo, Internet rappresenta un pericolo: navigare in un sito poco raccomandabile può significare consegnare il nostro PC nelle mani di un malintenzionato.

Cosa possiamo fare allora per navigare in sicurezza? Ci vuole molta attenzione e qualche accorgimento tecnico:

- Non navigare in siti palesemente sospetti, come siti per il download di materiale pirata (musica, video, ecc): la maggior parte dei virus si trova proprio qui.
- Prestare attenzione all'indirizzo di navigazione: una tecnica molto comune chiamata **typosquatting**, prevede di usare nomi di siti simili a quelli originali, con scopi fraudolenti (ad esempio www.appple.com al posto di www.apple.com).
- Fare molta attenzione quando, navigando in un sito, ci viene chiesto di fare qualcosa: ad esempio installare un aggiornamento o un software, cliccare "sì" o "no" in una finestra di pop-up. Talvolta queste richieste appaiono come delle minacce, è una tecnica molto usata. Ecco alcuni esempi di pop-up fraudolenti:

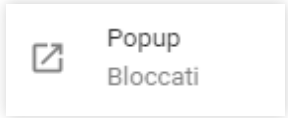
Di fronte a tutte queste minacce, oltre che al buon senso, dobbiamo affidarci alla tecnologia attivando delle impostazioni nel nostro browser allo scopo di difenderci da questo tipo di attacchi:

- Avere un antivirus nel proprio PC sempre aggiornato
- Attivare i controlli di sicurezza nel browser



- Non consentire automaticamente l'uso di periferiche del tuo PC ai siti dove navighi

- Tenere sempre attivo il blocco dei pop-up



PASSWORD SICURE

Consapevolezza, una buona dose di attenzione e alcune corrette abitudini sono le nostre difese contro gli attacchi informatici. Vediamo alcuni consigli per costruire uno scudo con cui difendere i nostri dati e quelli della nostra azienda.

Le **credenziali di accesso**, cioè lo username e la password, rappresentano la chiave per accedere al nostro mondo digitale. La password deve essere custodita gelosamente, essere impossibile da rubare o da indovinare. Il rischio che si corre è che altri possano accedere ai nostri dati o compiere azioni a nostro nome.
Come possiamo fare quindi per tutelarci?

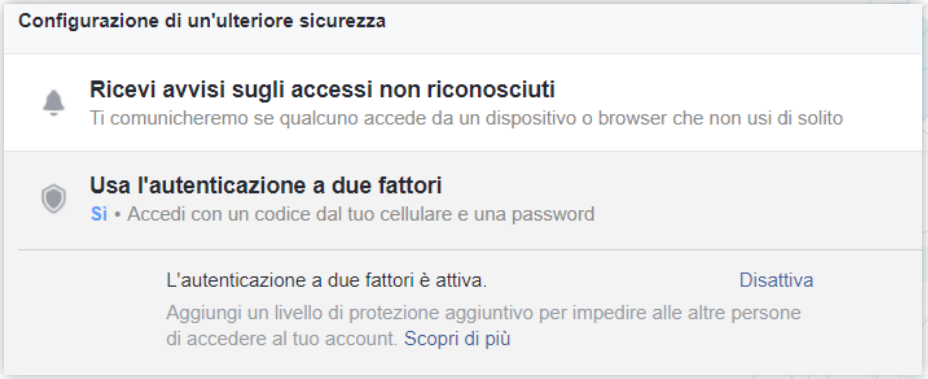
- Non usiamo password banali: nome e cognome, la parola "password", "1234" o "qwerty".
- Tieniamo a mente che gli hacker usano sistemi automatici e dizionari elettronici per trovare tantissime password in pochi secondi. Evitiamo quindi di utilizzare nomi di persone, cose o animali, anche se seguiti da numeri o simboli speciali: non è una complessità sufficiente.

Proviamo invece a creare password lunghe, ma facili da ricordare:
AMarioPiaceLaCioccolataBianca!

Oppure, creaimo un'apparente complessità: ad esempio Mario Rossi, nato il 10-04-1959 potrebbe avere questa password:
M1a0r0i4oR1o9s5s9i

Ricordiamo inoltre di modificare sistematicamente le nostre, almeno una volta all'anno.

Molti siti, banche on-line, social network, consentono di attivare un ulteriore livello di autenticazione: "**Strong authentication**" che prevede l'invio di un codice su telefono al momento dell'accesso. Questo è un metodo molto sicuro che è sempre bene attivare:



Differenziamo le password per i vari servizi/siti web, distinguiamo le password di lavoro da quelle usate nella vita privata.

SUGGERIMENTO

Creiamo tre tipologie di password:

1. *una per l'ambito lavorativo: e-mail, applicazioni aziendali, PC, ecc.*
2. *una per siti dove vanno inserite informazioni importanti e dati sensibili: e-commerce, social network, prenotazioni on-line, ecc.*
3. *un'altra ancora per siti di pura consultazione: forum, riviste on-line, siti cioè dove non forniamo informazioni di noi stessi. In questo caso la password potrà essere anche meno complessa.*

CURIOSITÁ

A fine 2017, un gruppo di hacker ha pubblicato un elenco di username, password ed e-mail di utenti rubate da siti di primaria importanza quali social network, servizi cloud, piattaforme di gaming on-line e molti altri.

Questo database è diventato una risorsa fondamentale per gli hacker di tutto il mondo perché contiene un numero molto elevato di credenziali: 1,4 Miliardi!!!!
Sapete quali sono le più comuni?
"123456", "123456789", "qwerty," "password" e "111111".

WI-FI

Siamo abituati ad essere sempre connessi e quando non ci troviamo a casa o in ufficio spesso cerchiamo una rete **Wi-Fi** pubblica.

Ma siamo sempre sicuri che questo accesso Wi-Fi sia legittimo e non sia stato creato per intercettare le nostre comunicazioni?

Immagina che io sia un hacker e che mi trovi con il mio PC in prossimità del ristorante "Maria Rosa": in pochissimo tempo e senza particolari attrezzature, creo un finto accesso Wi-Fi: "MariaRosa-free-wifi". Da quel momento potrò spiare tutte le comunicazioni di chi si connette e magari tentare di accedere ai loro sistemi.

Attenzione quindi: se devi accedere a Wi-Fi pubblici, cerca un cartello che indichi qual è la rete Wi-Fi ufficiale, oppure chiedila a qualcuno.

Ecco alcune regole da seguire quando ci si connette ad una rete Wi-Fi:

- Non comunicare mai informazioni importanti quando si è connessi ad un Wi-Fi pubblico.
- Non fare transazioni bancarie.
- Verificare che i siti sui quali navighiamo usino la cifratura HTTPS, stessa cosa per i sistemi di chat e messaggistica.
- Disabilitare la funzione di connessione automatica alle reti Wi-Fi.

MOBILE SECURITY: LA NAVIGAZIONE DA SMARTPHONE E TABLET

Lo **Smartphone** è diventato parte integrante della nostra vita ma è difficile rendersi conto di quante informazioni importanti vi siano contenute: le foto, i profili social, l'home banking, le App per gli acquisti on-line, ma anche la posta elettronica (privata ed aziendale), la VPN per connettersi in azienda e così via.

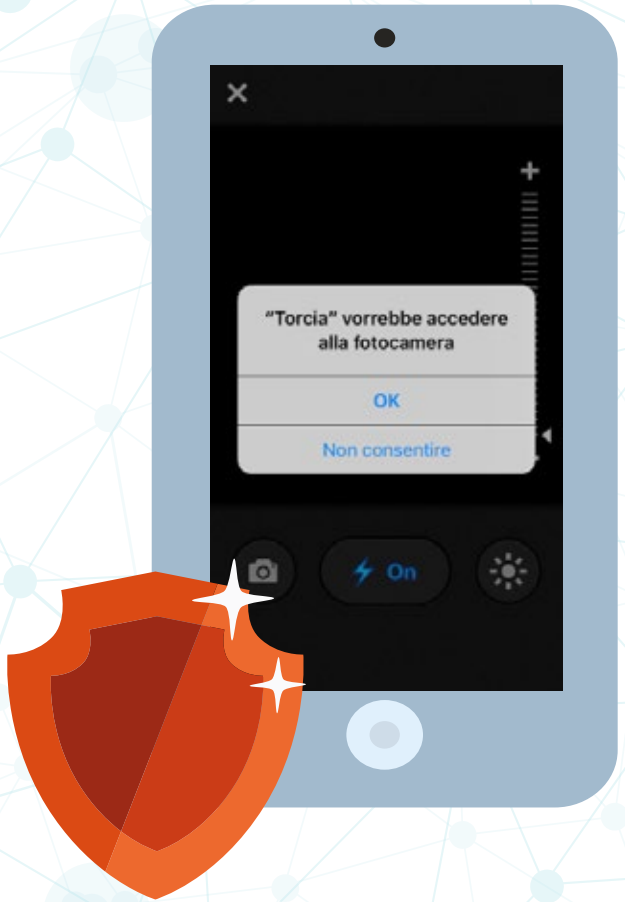
Sempre più spesso le App, memorizzano le nostre credenziali di accesso, così da non doverle inserire ogni volta.
Uno degli errori più frequenti connessi all'uso dei dispositivi mobile è quello di non impostare nessuna forma di protezione all'accesso, un PIN, l'impronta digitale, ecc.

È necessario quindi adottare alcuni accorgimenti che permettano di proteggere quanto contenuto all'interno dei nostri smartphone e tablet:

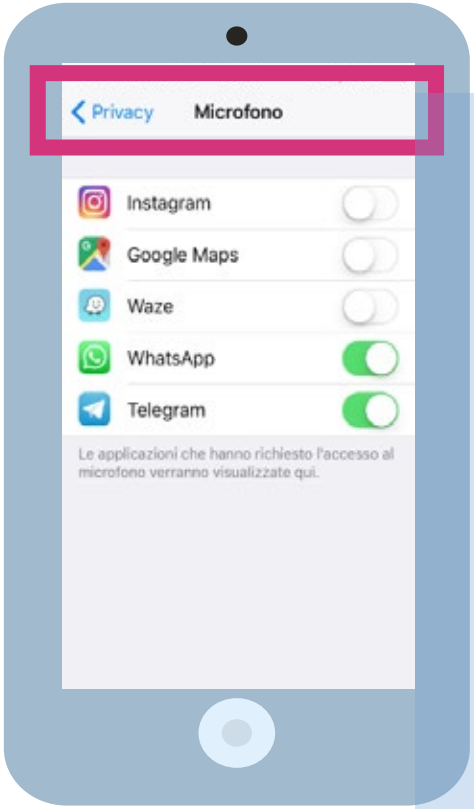
- abilitare il blocco automatico del dispositivo;
- attivare una forma di autenticazione per lo sblocco: PIN, impronta digitale o biometrica, swype;
- abilitare il servizio di cancellazione da remoto in caso di furto.

Ricorda inoltre di installare un Antivirus sui dispositivi mobile (ve ne sono anche di gratuiti). Esistono infatti virus sotto forma di App o inseriti all'interno dell'App stesse, quindi:

- usa sempre gli store ufficiali per scaricare un'App;
- quando installi un'App prenditi del tempo per leggere cosa fa (quali azioni comporta, cosa viene richieste, ecc.);

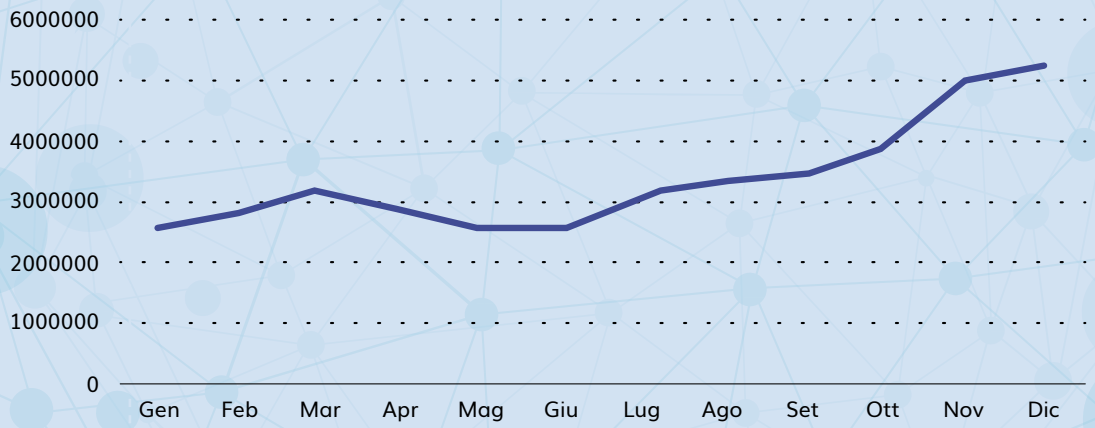


- ogni tanto rivedi le impostazioni sulla privacy e verifica quali App usano determinate funzioni dello smartphone.



CURIOSITÁ

La crescita dei virus per smartphone è inarrestabile, solo nel 2016, da Gennaio a Dicembre il numero di casi rilevati è raddoppiato!



SOCIAL NETWORK

I **Social Network** sono diventati la nuova frontiera della comunicazione, e di conseguenza, hanno attirato anche l'interesse dei cybercriminali, che vedono in queste piattaforme un'opportunità per raggiungere i loro scopi. All'interno dei social raccontiamo la nostra vita, fornendo quindi degli spunti interessanti.

Un esempio è la costruzione di mail di phishing partendo da un post pubblicato. Se ad esempio condivido che sto partecipando ad un convegno, l'hacker potrebbe inviarmi una mail fraudolenta con le slide dell'evento allegate.

Utilizzando i social network è bene tenere in considerazione queste buone pratiche:

- racconta di te, dei tuoi interessi, ma ricorda sempre che non sai chi ascolta i tuoi racconti;
- non lasciare il profilo dei social completamente "pubblico": prenditi del tempo per rivedere le impostazioni sulla privacy;
- diffida di giochi o test on-line che chiedono informazioni su di te e sulle tue abitudini;
- se un post porta il nome di un tuo amico, ma ti appare strano, potrebbe trattarsi di un furto di identità: è bene quindi stare attenti e notificarlo al tuo amico.

A ggiorna il sistema operativo e installa un antivirus anche sullo smartphone

B locca pop-up e richieste di siti sospetti

C ontrolla attentamente il dominio dei siti web

D edica tempo alla creazione di password sicure

E samina tutti gli elementi di una e-mail... riconosci i campanelli di allarme!

AGGIORNA IL SISTEMA OPERATIVO E INSTALLA UN ANTIVIRUS ANCHE SULLO SMARTPHONE

La prima protezione è l'attenzione e un po' di diffidenza, ma anche la tecnologia ci aiuta:
Tieni sempre aggiornato il **sistema operativo**...

... e il **browser**!
Internet Explorer, Edge e Chrome si aggiornano automaticamente.
Per gli altri browser è necessario verificare la procedura di aggiornamento e renderla il più possibile automatica.

Installa un **Antivirus** sul PC e sullo Smartphone!

Ecco alcuni antivirurs gratuiti:
https://www.avg.com disponibile anche per Android
https://www.avast.com disponibile anche per Android e iOS
https://www.avira.com disponibile anche per Android e iOS

B LOCCA POP-UP E RICHIESTE DI SITI WEB SOSPETTI

Non inserire credenziali se il sito non è protetto!

Se navigando in un sito poco conosciuto appaiono dei pop-up o delle richieste particolari, meglio abbandonarlo immediatamente.

C ONTROLLA ATTENTAMENTE IL DOMINIO DEI SITI WEB

Talvolta l'estensione di un sito web sembra corretta ma in realtà contiene un "inganno". Ecco alcuni esempi:

www.sitoweb.it	Se sto cercando "sitoweb" direi che questo è il sito giusto!
www.it-sitoweb.it	it-sitoweb.it è diverso da sitoweb.it .... Uno dei due domini potrebbe essere di proprietà di un hacker.
www.siloweb.it	Attenzione! Questo si chiama "*typosquatting*": ad uno sguardo frettoloso può sfuggire l'uso della "l" al posto della "t".
www.62.134.56.7	L'uso dei numeri (indirizzi IP) può indicare che il sito non è stato creato con attenzione e può celare un'intenzione malevola.
www.sitoweb.it/ajion5fhe43	Anche se appaiono numeri e cifre strane, l'importante è che siano dopo lo "/" e non prima.
sitoweb.it/eng	Non sempre i siti usano "www", ma questo non indica necessariamente che il sito sia malevolo.

D EDICA TEMPO ALLA CREAZIONE DI PASSWORD SICURE

Non usare parole composte da pochi caratteri.

Piuttosto che una passowrd corta e molto complessa, meglio una password lunga ma facile da ricordare:
A5tG!£d: sì, ma è difficile da ricordare;
AMePiaceFareColazioneConIBiscotti: sì, lunga ma facile da ricordare.

Se decidete di riusare la stessa password su diversi portali e applicazioni, definite almeno 3 livelli:
1: password di lavoro
2: password per siti di e-commerce e social network
3: altro

Ricordare tutte le password può essere talvolta snervante.
Provate ad usare dei programmi che vi aiutino:

Universal Password Manager
https://sourceforge.net/projects/upm/

Keepass
https://keepass.info/

E SAMINA TUTTI GLI ELEMENTI DI UNA E-MAIL. RI-CONOSCI I CAMPANELLI DI ALLARME!