DIGIWORKS

#30years #alwaysON

CYBER MINACCE IN AZIENDA

I 7 RISCHI INFORMATICI CHE OGNI IMPRENDITORE DEVE CONOSCERE

(E COME DIFENDERSI)

INDICE

DIGIWORKS, CHI SIAMO?

🚀 Dal 1995, Digiworks è il tuo alleato tecnologico di fiducia! Tutto è iniziato a Bitonto (BA), quando due appassionati di informatica, **Francesco Saracino** e **Lorenzo Coviello**, hanno deciso di trasformare la loro passione in una missione: aiutare aziende e professionisti a sfruttare al meglio la tecnologia. Oggi siamo molto più di una semplice azienda IT: siamo il tuo **reparto IT in outsourcing**! Un team di esperti sempre pronti a semplificare la tua vita digitale, migliorare la produttività e proteggere i tuoi dati, il tutto senza farti perdere tempo prezioso.

🔧 Problemi con la tecnologia? *Noi li risolviamo.*
📈 Vuoi far crescere la tua azienda? *Noi ti diamo gli strumenti giusti.*
🛡️ Sicurezza, efficienza e innovazione? *È il nostro pane quotidiano.*

Se pensi che la tecnologia sia complicata, è solo perché non ci hai ancora conosciuto. 😉
💡 **Digiworks: la tecnologia che lavora per te!**

INTRODUZIONE

Il **sistema informatico** è diventato uno degli elementi fondamentali per il corretto funzionamento della nostra azienda, quindi perché non prendere le **giuste precauzioni**? Ogni azienda è minacciata continuamente da rischi che posso intaccare i sistemi informatici: guasti, incidenti, furto di dati e attacchi cibernetici.

Le conseguenze dei danni informatici sono molto rischiose, infatti le imprese colpite da perdite o indisponibilità dei dati, mettono in grave pericolo la loro operatività e l'immagine acquisita sul mercato. La fonte più importante di rischio per l'azienda è l'**inconsapevolezza**: molto spesso non si conoscono o si sottovalutano i rischi informatici e quindi si diventa inevitabilmente vulnerabili. I dati rivestono un'importanza vitale per l'azienda e perderli o danneggiarli può causare danni molto gravi. Per questo abbiamo creato questa piccola guida che ti aiuterà a porre più attenzione a quelle attività giornaliere che riteniamo innocue, ma che in realtà nascondono diversi pericoli.

E-MAIL

QUALI RISCHI UN IMPRENDITORE PUÒ EVITARE?

Origini e significato

Partiamo dalla provenienza della parola "*mail*". È utilizzata oramai in tutto il mondo, proviene dall'inglese e significa posta, corrispondenza, non è raro in qualche film ritrovarla scritta all'esterno delle case americane sui contenitori della corrispondenza cartacea. Nel corso degli anni non abbiamo mai smesso di fare corrispondenza, abbiamo solo cambiato il mezzo e la velocità con cui farlo con una importante differenza: la comunicazione di uno a molti anziché uno ad uno, infatti in una mail posso scrivere contemporaneamente a più persone.

Quando e perché è nata?

Nel 1971 grazie ad un'azienda americana, la **A.R.P.A.N.E.T.** (Advanced Research Projects Agency Network) ed il suo referente, Ray Tomilson, a cui venne affidato un progetto del Ministero della Difesa statunitense il cui obiettivo era quello di **velocizzare la comunicazione tra diversi reparti** (il progetto che ora ha il nome di Internet), nacque così la e-lectronic Mail → e-mail. Oggi, diffusa comunemente come "mail", *ha cambiato enormemente il panorama delle comunicazioni mondiali*, ogni giorno ne vengono inviate e ricevute milioni in tutto il mondo.

Come si riconosce un indirizzo mail?

Tutti sanno che una mail è composta da una prima ed una seconda parte separate dal simbolo "@". La prima parte viene definita **nome utente**, cioè il nome della persona o riferimento: es. "mario.rossi@xxxx.it" oppure acquisti@xxxx.it;
nella seconda parte invece troviamo il **dominio** che viene registrato da un provider. Alcuni esempi di provider gratuiti sono: *Gmail*, *Yahoo*, *Libero*, *iCloud*, *etc..*, per dare un'idea di professionalità si può acquistare un dominio personalizzato presso i provider che offrono il servizio di registrazione dominio.

E-Mail e registrazione – 3 errori comuni

I tre clamorosi errori dell'e-mail professionale. Per un libero professionista o un'azienda l'e-mail è un vero e proprio strumento di lavoro, quindi perché i liberi professionisti commettono (quasi) tutti gli stessi errori?

- **Errore n. 1:** scegliere una casella e-mail *non personalizzata* (ad esempio mario.rossi@gmail.com). L'errore non è scegliere tra questo o quel provider (Gmail, e-mail, Yahoo, Alice, ecc), l'errore è quello di **rinunciare ad una e-mail personalizzata che trasmetta autorevolezza e professionalità** (es. mario.rossi@studiorossi.it). Facciamo un esempio: ipotizziamo che ci siano due avvocati ed i loro indirizzi e-mail sono rispettivamente:
  - andrea.rossi@gmail.com
  - marco.bianchi@studiolegalebianchi.it

Qual è l'indirizzo e-mail più professionale ed autorevole? Questo concetto è applicabile a qualsiasi tipologia di business.

• **Errore n. 2:** *concentrare tutti i messaggi di posta elettronica, quelli privati e quelli professionali, su un'unica e-mail.* In questo caso invece andiamo a danneggiare la nostra produttività. La gestione di una casella di posta elettronica che è intasata di messaggi danneggia la concentrazione e rende praticamente impossibile ritrovare i messaggi importanti.

• **Errore n. 3:** *sfruttare lo smartphone per leggere al volo i messaggi ed aspettare di rientrare in ufficio per rispondere alle e-mail con il tuo computer.* La posta elettronica è la seconda attività "brucia tempo", viene subito dopo le telefonate; con una corretta gestione/programmazione puoi rispondere al volo direttamente con il tuo smartphone, senza dover rinviare nulla.

Key Sensitive

Molti non sanno invece che gli indirizzi mail non sono "*key sensitive*", ovvero **non sono sensibili alle maiuscole e minuscole**, quindi possono essere scritte sia in MAIUSCOLO sia in minuscolo senza compromettere l'invio e la ricezione della mail stessa. **Ricapitolando, avere un indirizzo e-mail personalizzato ha tre vantaggi: aumenta l'autorevolezza percepita dai clienti; consente di mantenere separate le e-mail personali dalle e-mail professionali;**

semplifica la gestione della e-mail professionale in contemporanea su più dispositivi come tablet e smartphone.

Rischi reali di una mail

Affermiamo quindi che la mail è uno degli strumenti di comunicazione più utilizzato sia tra aziende e professionisti che tra componenti della stessa azienda come comunicazioni interne. Da quando si è affermata sul mercato la Apple con gli Iphone e successivamente Samsung con gli Android, i produttori stessi hanno obbligato tutti i possessori di smartphone di attivarne una per creare un account per attivare il telefono. Essendo la mail lo strumento di comunicazione più diffuso al mondo tra aziende, professionisti, pubblica amministrazione, etc. esaminiamo i possibili rischi a cui quotidianamente si va incontro.

Prima Regola di Sicurezza

Sfatiamo un mito: **nessun antivirus è in grado oggi di intercettare e bloccare una mail infetta di nuova generazione che contenga all'interno un Cryptolocker** (*). O meglio non è in grado di controllare la tua volontà o il tuo istinto di aprirla. Questo non significa che gli antivirus non svolgano dell'ottimo lavoro, sono necessari ed utili, ma in alcuni casi non possono evitare che un link venga cliccato facendoti rimbalzare su un sito non sicuro e dannoso.

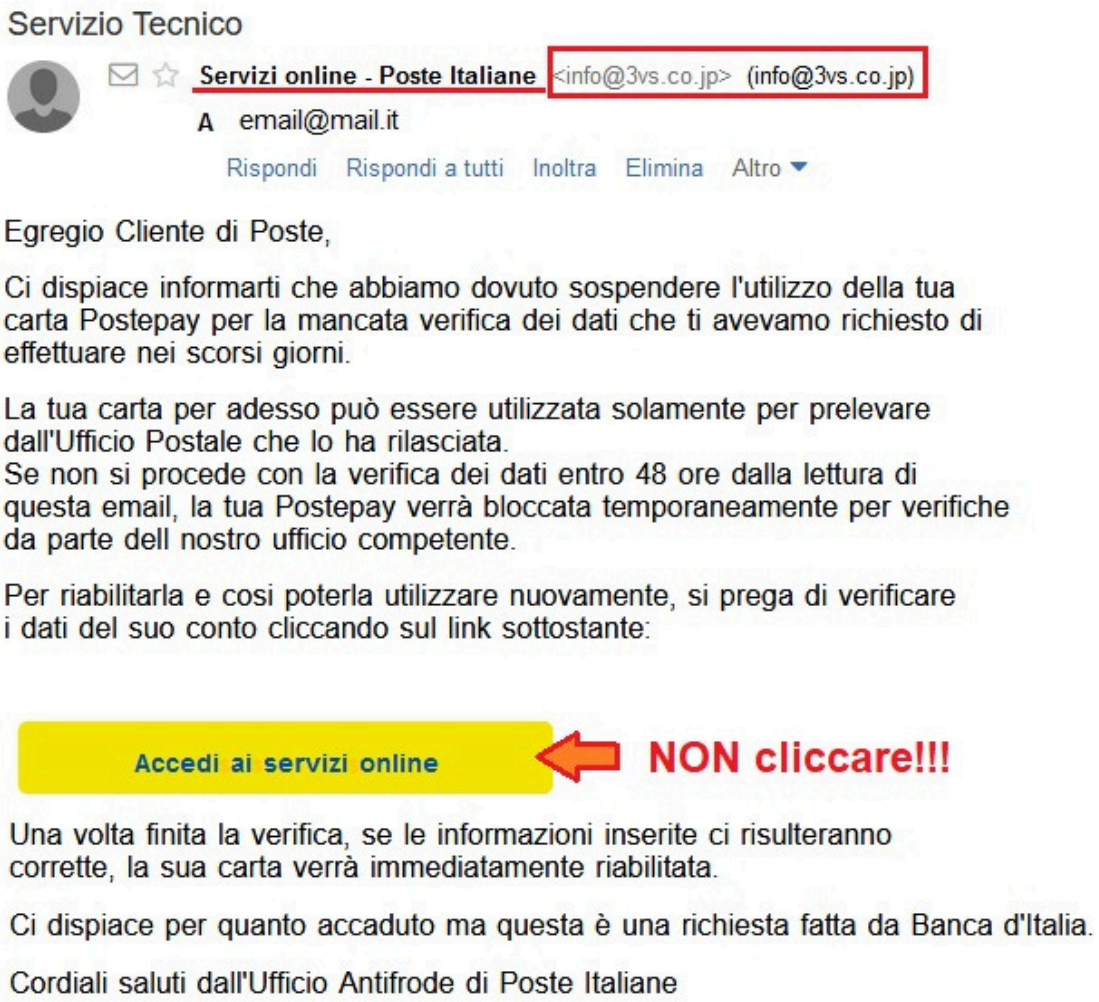
*Cryptolocker: criptazione/blocco dei documenti e dei dati con richiesta di riscatto in bitcoin.

Quindi la prima regola di sicurezza è: **rifletti prima di cliccare su un link di cui non sconosci la provenienza o di aprire allegati non conosciuti.**

Seconda Regola di Sicurezza

Diffida dalle mail che hanno come mittente te stesso o che si presentano a te con un nome utente a te conosciuto, la tua banca, il tuo conto postale o un tuo cliente o fornitore, ma che abbiano nell'indirizzo completo una sequenza di lettere non riconducibili al mittente a te noto.

Un esempio reale



In questo esempio chiaramente non è *Servizio online - Poste Italiane* che ha inviato una mail, né tantomeno è con una questa modalità che Poste Italiane richiede di aggiornare o inserire dati del conto corrente, password o codici legati alla carta di credito/bancomat. **Non è consigliato chiedere al mittente sospetto se la mail è veritiera, sarebbe come chiedere ad un falsificatore se le banconote che produce sono vere! Non ti fidare mai di questa tipologia di mail.**

Terza Regola di Sicurezza

Non cercare di aprire allegati che non si aprono con i normali software installati sui pc. Non seguire collegamenti esterni alle mail di cui non hai la certezza del mittente e non inserire dati sensibili in siti che sembrerebbero quelli a cui di solito accedi, ma che sono su indirizzo internet completamente diverso. **Non aprire file .zip allegati che contengono all'interno file di tipo "nomefile.exe", potrebbero essere virus sospetti e/o potrebbero installare software nascosti nel tuo pc che lo facciano diventare a tua insaputa un elaboratore di operazioni per il data mining** (*). In ogni caso aggiorna sempre l'antivirus, fai analizzare il file allegato prima dall'antivirus e munisci la tua rete internet di un firewall monitorato e gestito. Segui sempre la regola numero uno del buonsenso: se non ne sei convinto non aprirlo!

*data mining: insieme di tecniche e metodologie che hanno per oggetto l'estrazione di informazioni utili da grandi dati, datawarehouse ecc), quantità di dati (es. banche attraverso metodi automatici o semi-automatici).

Quarta Regola di Sicurezza

La posta in arrivo e quindi il suo contenuto possono essere modificati da un hacker se non usi un sistema di posta sicuro e con password sicura. Ti descriviamo un esempio reale di truffa: **sniffing, ossia il furto o intercettazione dei dati che hai nella tua posta in arrivo o nella posta di arrivo di un tuo cliente**.

Un nostro cliente, che chiameremo PD, utilizza un servizio di posta certificato con password sicura. L'azienda di PD si trova in Italia ma, per motivi lavorativi, ha rapporti frequenti con un'azienda tedesca a cui fornisce beni dopo averli revisionati. PD alla fine della revisione, come di consueto, invia all'azienda tedesca la fattura della prestazione specificando l'importo ed allegando regolare file pdf che presenta, come per la maggior parte delle aziende italiane, i dati bancari su cui procedere per il pagamento. L'azienda tedesca provvede al bonifico. Trascorsi 10 giorni, non c'era traccia del pagamento effettuato, eppure l'azienda tedesca aveva confermato la trasmissione... La soluzione arriva qualche giorno dopo quando, controllando la contabile del bonifico, si è riscontrata una inesattezza nel codice IBAN. L'IBAN, infatti, era stato modificato nella fattura ricevuta del committente tedesco, sprovvisto di un servizio di posta certificato... L'amministrazione della società tedesca non ha esitato ed effettuare il pagamento, peccato che sia stato fatto su uno sconosciuto conto tedesco.

Tecnicamente, cosa è accaduto?

La posta in arrivo del committente tedesco era oggetto di *sniffing**. La mail dall'Italia era corretta ed è ancora corretta nella posta inviata dell'azienda di PD, ma durante la trasmissione colui che era in modalità di ascolto "sniffing" ha intercettato la mail, modificato l'allegato con le coordinate del proprio conto ed ha proseguito con l'invio della mail.

Verifica sempre l'IBAN del tuo destinatario, soprattutto se c'è una variazione rispetto a quello su cui sei solito inviare pagamenti.

In caso di modifiche non richiedere approvazione o conferma del nuovo IBAN tramite mail perché chi è in ascolto "sniffing" risponderà confermando la variazione.

Ti consigliamo di chiamare il diretto interessato ricevere le conferme di cui necessiti.

PEC: Evoluzione della e-mail Circa 13 anni fa venne istituita in Italia la PEC: una mail con valore legale di consegna pari ad una Raccomandata con ricevuta di ritorno. Inizialmente fu lanciata per certificare il rapporto tra reparti della pubblica amministrazione, oggi il suo uso si è diffuso anche tra aziende private. Per la PEC i rischi sono gli stessi che per le normali mail!

*sniffing : intercettazione passiva di dati che transitano un una rete

Perché dovrei fare tutto ciò?

Spesso sentiamo dire dagli imprenditori: *"A me non è mai capitato"* Non è sufficiente come assunto per non intraprendere o iniziare ad avere accorgimenti utili ad evitare il peggio per la tua azienda in caso di mail dannose.

Non sai come fare?

Se non sai da dove iniziare non c'è nessun problema. **Possiamo aiutarti mettendo a tua disposizione la nostra conoscenza ed esperienza per attuare tutte le azioni preventive in caso di mail dannose!**

BACKUP
QUANTO SONO AL SICURO I TUOI DATI?

Sei riuscito a finire il lavoro per il quale hai investito diverse ore del tuo tempo, salvi tutto sul tuo computer e felice torni a casa per il lavoro svolto. Il giorno dopo torni e magicamente il tuo computer non si accende più e pensi a quanto i computer ti complichino la vita oggigiorno. Niente di più vero se non li utilizzi con estrema attenzione. Ciò di cui vorrei parlarti oggi sono proprio i backup!

Cos'è un backup?

Ti starai domandando, molto probabilmente cos'è un backup. **Un backup non è nient'altro che il salvataggio di una copia di un file o di un insieme di file fino a quel determinato momento storico.** Da qui puoi comprendere quanto essenziale è l'utilizzo dei backup nel tuo quotidiano Il concetto di backup è applicabile a tutto quello che riguarda il tuo computer. Esso è un aspetto fondamentale della gestione del computer. **È importante che tu cominci ad applicare questo concetto nel tuo quotidiano il prima possibile. .**

"Proteggere i dati oggi significa proteggere il futuro della tua azienda domani."

Come eseguo un backup?

Eseguire un backup è molto semplice. Come ti anticipato prima, si tratta semplicemente di una copia del file o del gruppo di file che vuoi mettere al sicuro. Pertanto, starai pensando: “Mi basta semplicemente duplicare il file in questione ed il gioco è fatto!”. La risposta è vera in parte, ma la domanda che seguirebbe dopo è: “Dove risiederà questa copia?” Questa è una domanda fondamentale, poiché se domani il tuo computer non dovesse accendersi più, sia il file originale che la tua copia non saranno probabilmente più accessibili.

La regola del 3-2-1

Per risolvere la problematica, esiste una regola denominata del 3-2-1, la quale ci consiglia di eseguire **almeno tre copie** in presenza di dati di rilevante importanza. **Due di queste copie risiederanno in locale sul tuo computer. Quella rimanente, invece, risiederà in cloud,** un posto esterno protetto da problematiche come quella indicata appena sopra.
Se non sai cos’è un cloud, ti basterà sapere che è un computer che risiede in un luogo sicuro e tenuto sotto controllo da tecnici specializzati.

Ma è davvero necessario tutto questo?

Potresti domandarti se tutto questo sia davvero necessario per essere sicuro che i tuoi dati restino integri ed affidabili. La risposta è sì: la regola spiegata è un ottimo punto di partenza per salvaguardare il tuo lavoro senza correre il rischio di perdere i tuoi preziosi dati.

Voglio proteggere i miei dati

Se vuoi proteggere i tuoi dati, puoi cominciare dai piccoli consigli riportati in questa breve guida ai backup.

I consigli spiegati in questa guida sono più che adatti per un'azienda che non necessita di mettere al sicuro una grande quantità di dati.

Ti consigliamo, però, di consultare un esperto per la gestione di molti dati: potrebbe fornirti maggiore sicurezza da eventuali attacchi informatici che possono bloccare la tua intera azienda e provocarti grosse perdite economiche.

"Un sistema senza protezione è come una casa senza serratura: prima o poi, qualcuno entrerà."

Lo sapevi che...

...Nel momento in cui diamo a qualcuno la password del wi-fi per accedere alla nostra rete, stiamo aprendo le porte ai virus che potrebbero essere presenti su smartphone e PC?

Come si mette al sicuro una rete senza fili?

La domanda è più che lecita in tempi in cui proprio le reti senza fili stanno diventando lo standard sia a livello privato che Enterprise.
Tempi complicati in cui la gestione degli accessi e delle password sta conoscendo falle e rovesci clamorosi.
Il tema è duplice, da una parte un'utenza soprattutto professionale, ormai abituata a pretendere di essere collegata, ad alta velocità, ovunque, comunque e spesso a costo di rinunciare a qualche dato e alla propria privacy. Dall'altra parte un universo di Cybercriminali che conosce al meglio questo campo e, puntualmente, usa queste conoscenze a proprio vantaggio per rubare informazioni, sottrarre identità, denaro, informazioni critiche e facendo ovviamente danni irreparabili.

Le 6 regole per proteggere le reti senza fili

Sperando di fare cosa utile, abbiamo pensato di indicare qui di seguito, **le 6 regole che secondo i più importanti esperti di sicurezza, bisogna assolutamente rispettare per cercare di mettere al sicuro la propria rete Wi-Fi aziendale e privata.**

1ª Regola: Usate bene la crittografia

Alcuni *Access Point Wi-Fi* offrono ancora lo standard di protezione WEP oggi fondamentalmente superato.
Gli hacker possono infatti entrare in una rete protetta da WEP utilizzando una suite di Hacking in pochi minuti. Per evitare intrusioni, è essenziale utilizzare quindi una variante. La *Wi-Fi Protected Access* (WPA), sia WPA che il più recente standard WPA2 (o WPA3 quando sarà possibile). Alcuni router Wi-Fi offrono poi una funzionalità denominata *Wireless Protect Setup* (WPS) che fornisce un modo semplice per collegare i dispositivi a una rete wireless protetta WPA. Un sistema pratico che però può essere sfruttato dagli hacker per recuperare la password WPA, quindi è importante disabilitare WPS nelle impostazioni del router. Nelle organizzazioni più grandi, ha più senso usare WPA in modalità Enterprise, che consente a ciascun utente di avere il proprio nome utente e password per connettersi alla rete Wi-Fi.
Ciò rende il Wi-Fi e gli accessi molto più facili da gestire quando i dipendenti escono regolarmente, in quanto puoi

semplicemente disabilitare gli account degli ex dipendenti; ma per utilizzare WPA in modalità aziendale è necessario appoggiarsi ad un server, noto come server RADIUS, che memorizza le informazioni di accesso per ciascun dipendente.

2ª Regola: utilizzare una password WPA sicura

Siamo al cuore della vicenda, uno dei temi più critici. Occorre infatti assicurarsi che qualsiasi password (o Passphrase) che protegge la propria rete Wi-Fi sia *lunga e casuale*, in modo che non possa essere facilmente intercettata da un hacker determinato.

È fin troppo facile configurare qualsiasi apparecchiatura con le sue impostazioni predefinite, in particolare perché il nome e la password di amministrazione predefiniti sono spesso stampati sul router stesso per consentire un accesso e un'impostazione rapidi. Ciò significa che gli hacker proveranno innanzitutto questi per accedere alla vostra rete. La modifica del nome di accesso e della password renderà più difficile l'accesso a un criminale. Sembra una banalità ma, soprattutto, in Italia... purtroppo non lo è. È possibile testare la sicurezza della propria rete protetta WPA, senza rivelare la propria password o Passphrase, utilizzando alcuni servizi ad hoc. Vi verrà chiesto di fornire alcuni dati, gli stessi dati che un hacker potrebbe acquisire o "annusare" in aria con un laptop da qualsiasi punto della vostra rete, e il servizio tenterà di estrarre la tua password.

Se il servizio non ha successo, è improbabile che un hacker abbia successo. Ma se il servizio trova la vostra password, allora sapete che dovete sceglierne una più lunga e più sicura. Tenete a mente che anche lo standard di sicurezza WPA2 difficilmente resisterà a un gruppo di hacker o ad un hacker ben organizzato ed ostinato.

3ª Regola: Controllare e scovare gli Access Point Wi-Fi non autorizzati

Gli Access Point anomali presentano un enorme rischio per la sicurezza. Questi non sono gli Access Point Wi-Fi "ufficiali" della vostra azienda, ma sono stati introdotti dai dipendenti (forse perché non possono ottenere un buon segnale Wi-Fi nel loro ufficio) o in teoria, dagli hacker che sono entrati nel vostro edificio e in maniera discreta lo hanno collegato a un punto Ethernet di nascosto.

In entrambi i casi, gli Access Point anomali rappresentano un rischio perché non si ha alcun controllo su di essi o sul modo in cui sono configurati: ad esempio, uno potrebbe essere impostato per trasmettere l'SSID, l'identificatore di 32 caratteri per una rete wireless, e consentire a chiunque di connettersi senza fornire una password.

Per rilevare gli Access Point non autorizzati è necessario eseguire regolarmente la scansione degli uffici e dell'area circostante utilizzando un laptop o un dispositivo mobile dotato di software adeguato come Vistumbler, uno scanner di rete wireless, o Airodump-ng.

Questi programmi consentono al computer portatile di "sniffare" le onde radio per rilevare qualsiasi traffico wireless che si sposta da o verso un Access Point non autorizzato e consente di identificare dove si trovano.

4ª Regola: Avere una rete separata per gli ospiti

Se si desidera consentire ai visitatori di utilizzare il Wi-Fi, è consigliabile offrire una rete ospite. Ciò significa che possono connettersi a Internet senza accedere alla rete interna della vostra azienda. *Questo è importante sia per ragioni di sicurezza, sia per impedire che possano inavvertitamente infettare la vostra rete con virus o altro Malware.* Un modo per farlo è utilizzare una connessione Internet separata con il proprio Access Point wireless. In realtà, ciò è raramente necessario in quanto i router wireless più commerciali e molti più recenti hanno la capacità di gestire *due reti Wi-Fi contemporaneamente*: la rete principale e un'altra per gli ospiti, spesso con l'SSID "*Ospite*". Ha senso attivare la protezione WPA sulla rete ospite, piuttosto che lasciarla aperta, per due importanti motivi. Il primo consiste nel fornire un certo livello di controllo su chi lo utilizza: è possibile fornire la password agli ospiti su richiesta e, a condizione che vengano modificati frequentemente, è *possibile impedire che il numero di persone che conoscono la password aumenti troppo*. Ma ancora più importante, questo protegge i vostri ospiti da altre persone sulla rete ospite che potrebbero provare a curiosare nel loro traffico.

Questo perché, anche se utilizzano la stessa password WPA per accedere alla rete, i dati di ciascun utente vengono crittografati con una "chiave di sessione" diversa, che la rende sicura dagli altri ospiti.

5ª Regola: Nascondete il nome della vostra rete

Gli Access Point Wi-Fi sono solitamente configurati con impostazione predefinita per trasmettere il nome della rete wireless, noto come identificatore del set di servizi o SSID, per semplificare la ricerca e la connessione.
Ma l'SSID può anche essere impostato su "*nascosto*" in modo che un utente debba conoscere il nome della rete prima di poterci connettere.
Dato che i dipendenti dovrebbero conoscere il nome della rete Wi-Fi della vostra azienda, non ha senso trasmetterlo in modo che chiunque altro che passa di lì possa facilmente trovarlo. È importante notare che nascondere il vostro SSID non dovrebbe mai essere l'unica misura che prendete per proteggere la vostra rete Wi-Fi o quella dei vostri clienti, perché gli hacker che utilizzano strumenti di scansione Wi-Fi possono ancora rilevare la vostra rete e il suo SSID anche quando è impostato su "nascosto." **Ma la sicurezza consiste nel fornire più livelli di protezione e nascondendo il vostro SSID, o quello dei vostri clienti, potreste evitare di attirare l'attenzione degli hacker opportunisti, quindi è una misura semplice che vale la pena di prendere.**

6ª Regola: Utilizzare un Firewall

I **firewall hardware** forniscono la prima linea di difesa contro gli attacchi provenienti dall'esterno della rete, e la maggior parte dei router hanno firewall incorporati, che controllano i dati in entrata e in uscita e bloccano qualsiasi attività sospetta.
I dispositivi di solito sono impostati con impostazioni predefinite ragionevoli che garantiscono un lavoro decente. La maggior parte dei firewall esamina e capisce gli indirizzi di origine e destinazione. Queste informazioni vengono confrontate con un insieme di regole predefinite e/o create dall'utente e determinano se il pacchetto dati è legittimo o meno, quindi se deve essere consentito o scartato.
I firewall software di solito funzionano sul desktop o sul computer portatile, con il vantaggio di fornire un'idea migliore del traffico di rete che passa attraverso il dispositivo. Più che solo le porte utilizzate e dove i dati stanno andando, saprà quali applicazioni vengono utilizzate e può consentire o bloccare la capacità di quel programma di inviare e ricevere dati.
Se il firewall software non è sicuro su un particolare programma, può chiedere all'utente cosa dovrebbe fare prima di bloccare o consentire il traffico. **Per le aziende che dovrebbero avere una rete più strutturata, è necessario montare un Firewall hardware e farlo configurare da personale esperto.**

PASSWORD: SEMPLICE O COMPLESSA?

E’ meglio avere una password semplice che riesco a ricordare a memoria oppure una password complessa scritta su un bigliettino che lascio sulla scrivania? Beh, la risposta non risiede in nessuna delle due opzioni: come ben sappiamo **la verità sta nel mezzo**. Difatti sarebbe molto più intelligente creare una password semplice da ricordare ma allo stesso tempo complessa con all’interno numeri, lettere maiuscole e caratteri speciali.

Cos’è una password?

Prima di tutto, però vediamo cos'è una password e a cosa serve nell’ambito informatico. Una password è una sequenza di caratteri alfanumerici utilizzata per accedere ad una risorsa informatica. Solitamente è associata ad un nome utente o identificativo.

L’uso delle password risale ancor prima dell’era dell’informatica: essa veniva utilizzata molto in ambienti di spionaggio. Odierni comuni esempi di utilizzo di password li potete trovare nei servizi bancari che, probabilmente, utilizzate ogni giorno.

“Nel mondo digitale, la tua password è la chiave di casa: non lasciarla mai sotto lo zerbino.”

Norme di sicurezza elementari

Ora che abbiamo capito cos'é una password e perché dovremmo sceglierne una semplice da ricordare ma allo stesso tempo complessa, vi domanderete: **"Come ne creo una?"** Bene, con i semplici consigli che riporterò qui sotto, potrete avere una password che fa al caso vostro!

Prima Regola di Sicurezza

Nell'impostare una password, è sicuramente **sconsigliabile utilizzare informazioni ovvie** come ad esempio il vostro nome o cognome o persino altri dati anagrafici. Questo perché, basterebbe un minimo di studio su chi siete per poter risalire facilmente alla vostra password mediante l'uso di software dedicati!

Seconda Regola di Sicurezza

Ricordate sempre che più sarà corta la vostra password e più facilmente potrete essere a rischio! **Ogni singolo carattere aggiunto alla vostra password, la renderà molto più complessa.**

Terza Regola di Sicurezza

Cambiate periodicamente le vostre password e non utilizzate la stessa per ogni servizio che utilizzate!

Perché' dovrei fare tutto cio'?

Chiaramente potrete domandarvi il perché di tutto questa attenzione alle vostre password: probabilmente non avete mai avuto problemi in merito e pertanto le cose vi stanno bene così come sono! In realtà problematiche di questo tipo, legate alle password utilizzate sono veramente comuni e possono portare grosse perdite alla tua azienda!

Un esempio reale

Flipboard è uno dei più noti aggregatori di notizie, grazie al quale milioni di utenti dopo essersi registrati possono ritrovare notizie sincronizzate su tutti i proprio dispositivi. Qualche mese fa, Flipboard ha subito un furto di dati massivo dove le password di ben 145 milioni di utenti sono state rubate.

Qualora non seguiste la regola #3, sareste a serio rischio. Facciamo un esempio: siete iscritti a Flipboard e utilizzate la stessa password che utilizzate per il vostro online banking. Non avete l'abitudine di cambiare la vostra password e utilizzate la stessa su ogni servizio a cui siete iscritti. Capite bene che un utente malevolo potrebbe facilmente avere accesso alla vostra mail e persino al vostro online banking. **Come ricordo tutte le mie password?** Ci sono diversi servizi, in rete, molto sicuri e gratuiti che vi permettono di avere le vostre password in cloud, pronte all'uso.

Mettere le vostre password in queste enormi banche dati vi permetterà di avere:

1. Una password per ogni servizio;
2. Non dovrete necessariamente ricordare la vostra password a memoria;
3. Fare login con un semplice click nei vostri servizi;
4. E tanto altro...

Non sai come muoverti?

Se non sai ancora come muoverti, non c'e' nessun problema. **Possiamo aiutarti nel tuo percorso di creazione e gestione delle password, mettendo a disposizione la nostra conoscenza ed esperienza in merito!**

PROTEZIONE DALLA RETE ELETTRICA

Sfatiamo un mito, i gruppi di continuità economici non servono a niente!

Una breve spiegazione, pratica, delle tipologie di *Uninterruptible Power Supply* (UPS) o gruppo di continuità, che si possono scegliere nel proprio ambito applicativo.

Perchè la protezione dell'alimentazione è importante?

Al giorno d'oggi nessuna società può permettersi di lasciare le proprie risorse IT non protette da problemi di alimentazione, soprattutto quando annessi ci sono reparti produttivi, per i seguenti motivi: brevi interruzioni possono creare problemi; buchi o cali di alimentazione anche per 1/4 di secondo (interruzioni transitorie) possono innescare perdite di dati nel reparto IT tali da compromettere il flusso di informazioni da minuti a ore.

Il fermo negli uffici aziendali causa, con personale impiegato, costi in perdita notevoli. Peggio ancora quando alcuni dati passano dagli uffici al reparto produttivo per i programmi da eseguire nelle macchine o linee automatizzate in real time. La rete non fornisce tensioni "pulite": le variazioni di tensione possono causare guasti o portare apparecchiature in stato di standby, con conseguenti danni. Ciò non è dovuto esclusivamente al fornitore di energia, dipende anche dalla tipologia della

rete e dalla distribuzione nella propria zona e nel proprio impianto, anche se fosse presente una propria cabina elettrica.

La fornitura di rete non è mai garantita al 100%: le interruzioni di alimentazione dall'ente fornitore ci sono sempre state e ci saranno sempre, anche se meno frequenti.

E ciò è anche scritto nei contratti di fornitura che firmiamo.

Intensificazione del rischio di guasti: le apparecchiature IT ed elettroniche di oggi sono equipaggiate con componenti sempre più miniaturizzati, la gestione della qualità di alimentazione è quasi sempre scaricata sull'utente utilizzatore o sull'installatore, basta leggere almeno una volta un manuale di installazione, dal quale si intuiscono quali precauzioni sull'alimentazione sono richieste per il corretto funzionamento.

Generatori e soppressori di sovracorrente non sono sufficienti: i generatori di energia non si avviano istantaneamente ma generalmente dopo 10 secondi, non fornendo nessun tipo di protezione dai picchi di potenza a da qualsiasi altro disturbo elettrico.

I soppressori aiutano contro *spike* (picco) di tensione, ma non con i cali temporanei o di media durata, tantomeno con disturbi condotti in rete.

L'affidabilità è tutto: una volta la parte IT era di supporto all'impresa, oggi ne è parte integrante, complice la nuova digitalizzazione delle industrie, e la disponibilità è necessaria per il funzionamento di tutti i reparti.

Perché scegliere un UPS professionale?

Perché ha la parte di tensione di ingresso separata da quella di uscita. Ovvero l'energia elettrica entra, ricarica le batterie. Un circuito elettronico poi si occupa di prendere l'energia delle batterie, convertirla in ottima qualità e distribuirla alle apparecchiature IT.

Garantisce una tensione costante e una qualità di segnale eccellente. Non è solo un soccorritore momentaneo di tensione, è un vero e proprio strumento di protezione e garanzie per le apparecchiature.

Occhio all'aspetto batterie

Se possibile, scegliere UPS che montino batterie standard e sostituibili, in quanto a volte negli standby e line interactive economici si trovano batterie ricaricabili proprietarie o non facilmente reperibili in commercio, il cui costo come parti di ricambio è superiore al costo di un UPS nuovo.

Attualmente le batterie più diffuse e meno costose che si trovano in alcuni marchi di UPS sono le 7Ah 12VDC. Una nota sull'installazione degli UPS con batterie ricaricabili: non devono mai essere chiusi dentro armadietti non areati, ma sempre con un adeguato ricambio o a pavimento, con uno spazio libero attorno. Questo perché le batterie, seppur in valori modesti, possono emettere gas idrogeno che, miscelandosi all'aria, diventa una miscela esplosiva. Ciò è maggiormente vero quando si utilizzano UPS con gruppi batterie supplementari. Ai fini assicurativi potrebbe venire richiesto lo spostamento in luogo sicuro.

Quando sostituire le batterie

I fattori principali che influenzano la durata sono i cicli di carica/scarica parziale delle batterie, la temperatura dell'ambiente circostante, la qualità dell'elettronica di carica.
Le batterie all'acido che vengono installate negli UPS, hanno un ciclo di vita medio di 5 anni (standby use), poi vanno sostituite. In particolare, **la temperatura dell'ambiente dove è installato un UPS può influire negativamente sulla vita delle batterie:** sopra i 30°C si ha un declassamento e non è raro trovare batterie rigonfie con inizio di perdita dell'acido dopo tre anni di funzionamento. Altro fattore non trascurabile è dato dalla qualità delle batterie, ad esempio è facile trovare delle batterie a basso costo che, però, avranno un ciclo di vita inferiore ai 5 anni. In generale un buon consiglio basato sull'esperienza è una **sostituzione delle batterie ogni 3 anni**, perché è proprio dal terzo anno che si evidenzia un calo significativo della durata. Se invece l'UPS è stato sovradimensionato oltre il 40% del carico necessario, allora si può raggiungere la soglia dei 5 anni.

USB

Perché si utilizzano?

La risposta che riceviamo spesso dalle aziende è: “Per mettere al sicuro i nostri dati e per averne una copia” Vero. Sono un ottimo supporto temporale sul quale memorizzare file, cartelle, backup di gestionali...peccato che:

- anche se protette da password sono vulnerabili in caso di **smarrimento**;
- se dovessero cadere **potrebbero danneggiarsi** perdendo irrimediabilmente tutti i dati presenti all’interno;
- connettendosi da un pc all’altro potrebbero infettarsi con dei virus che vengono poi trasmessi a tutti i pc con i quali la chiavetta entra in contatto.

Sei ancora sicuro di volerle utilizzare per proteggere i tuoi dati?

Se la tua riposta è Si. Ritorna al paragrafo precedente e riprenditi i punti dopo il “peccato che..”

“La prima regola della sicurezza è la consapevolezza: se non conosci i rischi, sei già in pericolo.”

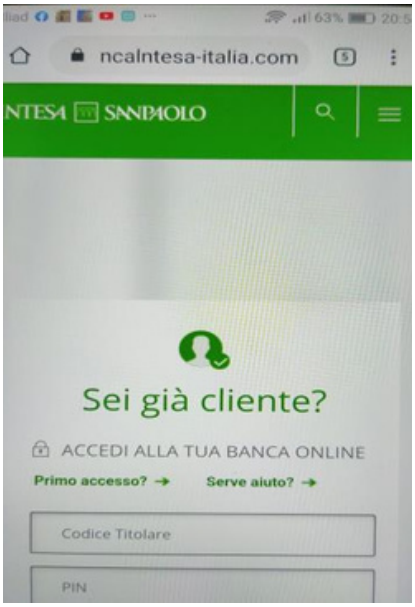
SMS

Quanto ancora si utilizzano?

Diciamoci la verità, per un periodo di tempo avevamo dimenticato completamente dell'esistenza degli *Short-Message-Service* (SMS).
Il servizio WhatsApp ci ha completamente catturati e fornito funzionalità a portata di mano di gran lunga superiori rispetto agli sms, contenendo notevolmente i costi per inviare immagini (gli SMS che contenevano immagini o suoni venivano addebitati come MMS). Oggi sono tornati alla riscossa! Non ne possiamo fare a meno, non come invio, ma come ricezione.
I servizi bancari, per esempio, inviano un messaggio in tempo reale per informare dei movimenti di spesa dal conto o dalla carta di credito. La banca invia anche codici di accesso per autorizzare operazioni sul conto corrente. Ed anche in questo caso i truffatori non hanno perso tempo ad organizzarsi, ecco a voi un **esempio di truffa tramite SMS**.

Se doveste ricevere un messaggio del genere dalla vostra banca, cosa fareste? Probabilmente presi dalla frenesia di tutti i giorni, avreste cliccato sul link.

Bene, dopo aver cliccato sul link la pagina che appare è la seguente.



Riconoscendo i colori, i simboli e l'impaginazione del sito della propria banca è istintivo inserire i campi richiesti, ovvero Codice Titolare e PIN.

Sappiate che da questo momento li avete consegnati liberamente ad un esperto Hacker che è già entrato nel vostro conto corrente in modalità "visualizzazione".

Vediamo la schermata successiva una volta compilati i campi richiesti.

Vengono richiesti i dati della vostra carta: scadenza, Cvv ed il vostro numero di telefono. **Adesso hanno tutto ciò di cui necessitano, ma siamo stati noi stessi ad aver trasmesso i dati.**

Il nostro consiglio è quello di non fidarsi degli sms che ti invitano a collegarti al tuo conto corrente, postale o bancario, per modificare le credenziali di accesso.
Su quei conti ci sono i tuoi risparmi, il frutto del tuo lavoro quindi fai molta attenzione a questa tipologia di SMS. Diffida da chi richiede queste informazioni con una telefonata, anche se hai ricevuto un messaggio di avviso o una chiamata.
Questi dati sensibili non vanno trattati in alcun modo al telefono! Sii prudente!

"La sicurezza informatica non è un costo, ma un investimento per la sopravvivenza della tua azienda."

CONCLUSIONE

Ti è stata utile la nostra guida?

Ci auguriamo che questa guida ti sia stata utile per migliorare la sicurezza informatica della tua azienda. Proteggere i dati e prevenire le minacce digitali è fondamentale per garantire continuità e affidabilità al tuo business.

🔹 Resta sempre aggiornato sulle ultime novità in ambito tecnologico! Seguici sui nostri canali online per ricevere consigli, approfondimenti e strumenti utili per migliorare la protezione del tuo sistema informatico.

📞 Hai bisogno di una consulenza personalizzata? Se vuoi verificare l'efficacia delle tue misure di sicurezza o hai dubbi sulla protezione dei tuoi dati, contattaci. Saremo felici di aiutarti a rendere il tuo sistema più sicuro ed efficiente.

🚀 La sicurezza informatica non è un lusso, ma una necessità!

📞 080 3740369
✉ info@digiworks.it

DIGIWORKS

#30years #alwaysON