ATTI DEL WEBINAR: INTRODUZIONE ALLA CYBERSECURITY

Ordine dei Periti Industriali e dei Periti Industriali Laureati della Provincia di Vicenza del 14/10/2021

1. PROTEZIONE DEI DATI E CYBERSECURITY

È considerato dato qualsiasi forma fisica o meno impiegata per rappresentare un fenomeno evento o fatto. La maggior parte dell'attività che svolgiamo quotidianamente sono accomunate dalla necessità di analizzare conservare e trasmettere dati. Acquistare con moneta elettronica scattare una fotografia spedire e-mail telefonare sono tutte operazioni che comportano il trasferimento o l'utilizzo di dati e informazioni. Tra i dati con cui entriamo quotidianamente in contatto alcuni possono richiedere una maggiore attenzione rispetto ad altri per via delle possibili gravi conseguenze derivanti dalla con loro compromissione dunque qualora i dati o gli stessi supporti con cui questi sono conservati diventano disponibili anche a soggetti non autorizzati. La compromissione dei dati può infatti portare a perdita irreversibile di informazioni con compromissione del segreto professionale o della proprietà intellettuale perdite economiche dirette, perdita di immagine.

2. DATI INFORMATICI E CYBER CRIME

Quando i dati sono conservati e trasmessi facendo uso di supporti digitali come server questi possono essere soggetti ad un maggior rischio di compromissione. La possibilità di realizzare un collegamento in modo istantaneo tra dispositivi e caratteristiche della rete informatica è il principale punto di forza ma anche un potenziale punto debole. Il termine inglese cyber crime comprende diverse categorie di crimini informatici tra cui le infrazioni contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici ma anche le infezioni legate alla violazione dei diritti d'autore della proprietà intellettuale del segreto professionale. La cyber security è quell'insieme di attività e strategie che permettono di proteggere i sistemi e reti dagli attacchi digitali rendendo la vita difficile a chi vuole impossessarsi dei nostri dati. Per raggiungere tali obiettivi è fondamentale che tutti gli utenti del sistema informatico comprendono e rispettino i principi di base per la sicurezza dei dati.

3. I DANNI DEL CYBER CRIME

In italia e in tutto il mondo, ogni anno, il cybercrime è causa di perdite economiche di decine di miliardi di euro, a causa di danni diretti e indiretti che in grado di provocare. Il fenomeno del cyber crime non e' solo causa di danni economici, ma può contribuire concretamente al rischio psico-sociale, tramite il suo impatto sullo stress lavoro correlato. Chi subisce o diviene complice suo malgrado di un crimine informatico può diventare vittima accuse ingiuste e può subire effetti riconducibili al disturbo da stress post traumatico.

4. LA CYBERSECURITY

Le principali categorie di attacco informatico sono:

- Truffe informatiche;
- Password cracking - ottenimento forzato di dati di accesso;
- Cyber estorsione - richiesta di denaro per evitare un attacco;
- Attacchi ransomware - richiesta di denaro in cambio del ripristino a seguito di attacco;
- Cryptojacking - utilizzo illecito delle risorse informatiche.

5. TRUFFE INFORMATICHE

L'espressione truffe informatiche descrive e comprende la maggior parte delle tipologie di attacco basate sullo sfruttamento della fiducia e/o dalla distrazione della vittima, che coopera su malgrado alla compromissione del dispositivo utilizzato installando ad esempio software malevoli.

Questo avviene, ad esempio:

- Realizzando applicazioni che, pur fornendo le funzionalità desiderate, forniscono accesso alla memoria del nostro dispositivo o inviano dati verso dispositivi di chi organizza l'attacco;
- Proponendo l'installazione di estensioni per browser o altri programmi malevoli nascondendo la richiesta di consenso ad istallazione in finestre dell'aspetto fraintendibile.

  Sebbene chi progetti queste tipologie di attacco confidi nella disattenzione dell'utente, queste riescono a colpire indistintamente sia i meno esperti che gli utenti più navigati. Proprio i più esperti possono essere i più vulnerabili, perché abitudine e assuefazione all'uso dei sistemi informatici possono portare più facilmente a comportamenti rischiosi. Bisogna aggiungere infine che alcune strategie di attacco si basano specificamente sull'assenza di effetti rilevabili dall'utente, sia nell'immediato che con il passare del tempo, motivo per cui la prevenzione è fondamentale. Sulla traccia degli esempi visti, una volta installato il programma malevolo, chi sta dietro l'attacco potrebbe quindi ricevere dati provenienti dal nostro dispositivo o assumerne il controllo. Tra i vari tipi di programmi malevoli vi sono i keylogger, che tracciano come interagiamo con il terminale, inviando dati verso altri pc (per es. Si possono ottenere dati come nomi utente e password di account).

6. PASSWORD CRACKING

Il password cracking consiste nell'uso di strategie di vario tipo per scoprire le credenziali di accesso ad un sistema informatico o ad un profilo utente. La metodologia di attacco in questo caso non prevede alcun tipo di collaborazione da parte di una vittima, ma si basa unicamente sul sottoporre al sistema informatico credenziali potenzialmente valide, fino a individuare quelle corrette. In entrambi i casi fin qui analizzati, la finalità dell'accesso malevolo è tipicamente economico diretto , magari anche mettendo in vendita tali dati, oppure al fine di impiegarli per altri usi illeciti, come:

- Spionaggio industriale
- Pirateria informatica
- danneggiamento dell'immagine del proprietario del sistema o dell'account sottoposto ad attacco o di altri soggetti cui si riferiscono i dati sottratti
- Furto d'identità.

7. CYBER ESTORSIONE E ATTACCHI RANSOMWARE

Cyber estorsione e attacchi ransomware sono molti simili, in quanto in entrambi i casi lo scopo che si prefigge l'organizzatore dell'attacco è quello di estorcere denaro al soggetto bersaglio. La differenza si trova principalmente nella tempistica con cui viene richiesta la somma di denaro alla vittima:

- Nel primo caso il criminale minaccia il proprietario del sistema sotto attacco, chiedendo di essere pagato per salvaguardare i propri dati;
- Nel secondo caso, il criminale rende impossibile l'accesso a tutti o parte dei documenti presenti sul sistema a cui è riuscito ad accedere, chiedendo un riscatto in denaro in cambio delle "chiavi" necessarie per ripristinare l'accesso ai file.

8. CRYPTOJACKING

Il cryptojacking è tra le forme di attacco più comuni, e potenzialmente si tratta di quella in apparenza più innocua. In questo caso, chi compie l'attacco informatico si limita ad occupare in modo abusivo una parte delle risorse informatiche hardware del sistema bersaglio, sfruttandole poi per trarne una qualche forma di profitto. Il termine cryptojacking deriva infatti dalla principale attività che viene svolta utilizzando tali risorse, ovvero lo svolgimento dei complessi calcoli richiesti per ottenere e gestire flussi di criptovalute. In questo caso i dati potrebbero restare intatti e disponibili, ma lo stesso non si può dire della funzionalità dei sistemi aggrediti. Maggiore sarà l'occupazione di risorse da parte del sistema di attacco, più evidente sarà l'impatto sulle prestazioni dei dispositivi che vengono sfruttati. In casi estremi, questo può portare a disservizi anche gravi, con conseguenti perdite economiche sia dirette che legate al danno d'immagine subito.

9. MISURE TECNICHE CONTRO IL CYBERCRIME

I sistemi informatici aziendali possono essere visti in modo del tutto analogo alla sede fisica dell'azienda. Chi volesse ottenere i dati contenuti negli archivi, o presenti sulla scrivania di uno dei lavoratori , avrà ottime possibilità di ottenerli soprattutto se in grado di introdursi nella sede. Inoltre, il danno sarà potenzialmente tanto più grave quanto maggiore sarà la sua libertà di movimento una volta all'interno. Cosa accadrebbe, se oltre ad ingressi ed uscite noti e sorvegliati fossero presenti anche altre porte secondarie, magari trascurate perché solitamente chiuse o ancor peggio dimenticate aperte da qualcuno? I programmi di applicazione utilizzati, così come gli stessi sistemi operativi presenti nei dispositivi impiegati per l'attività lavorativa, possono avere punti deboli equivalenti a questa porta trascurata o dimenticata aperta. Gli sviluppatori di software e sistemi operativi sono consapevoli di questa possibilità, e verificano con attenzione la possibile presenza di queste vulnerabilità. Ogni volta in cui queste vengono riconosciute, sono gli stessi sviluppatori a cercare ed applicare la soluzione più adatta per chiudere il varco per sempre, o almeno renderlo molto più resistente a tentativi di accesso. Questa attività porta alla realizzazione di aggiornamenti, la cui disponibilità viene indicata tempestivamente agli utenti o che vengono direttamente installati.

10. CONTROLLO DEGLI ACCESSI

Anche gli ingressi principali devono essere adeguatamente protetti con un sistema di controllo degli accessi che permetta di accedere solamente chi ne ha diritto, limitando l'accesso ad aree specifiche dove necessario. Sistemi e dispositivi informatici effettuano questi controlli assegnando ad ogni utente delle credenziali di accesso, tipicamente coppie di nomi/codici identificativi dell'utente e password oppure codici di sblocco. Non utilizzare questi sistemi significa lasciare la porta aperta, permettendo a chiunque abbia accesso fisico al dispositivo di ottenere accesso alla rete aziendale

11. FIREWALL

Utilizzando i firewall l'obiettivo è quello di impedire ogni comunicazione con la rete o attraverso la rete per particolari tipologie di dati oppure ai dati provenienti da o diretti verso determinati indirizzi. L'impiego di firewall può quindi impedire qualsiasi tipologia di comunicazione diretta con la rete ed i dispositivi aziendali ai potenziali malintenzionati, garantendo un livello di protezione aggiuntivo. Inoltre, con un firewall è possibile bloccare l'accesso a indirizzi e siti malevoli anche dall'interno della rete.

12. SOFTWARE ANTIVIRUS

I software antivirus sono indispensabili per garantire un'adeguata sicurezza contro software e programmi malevoli. Questi programmi sono sviluppati e continuamente aggiornati per riconoscere tempestivamente e impedire il funzionamento di codici pericolosi sul dispositivo dove sono installati.

13.PROTEZIONE DELLE RETI

Un controllo accessi può essere realizzato anche per il collegamento fisico alla rete aziendale, consentendo solamente ad alcuni dispositivi presenti di collegarsi ed eventualmente comunicare tra loro, bloccando invece qualsiasi tentativo di connessione a dispositivi non riconosciti e dunque potenzialmente non innocui ne sicuri. Particolare attenzione deve poi essere riservata alle reti wi-fi: se non protette, dunque prive di controllo per la connessione da parte di un dispositivo, le informazioni che vi transitano possono essere intercettate con relativa facilità, lasciando la possibilità ad un eventuale malintenzionato di ottenere i dati inviati o ricevuti attraverso queste comunicazioni, come codici di accesso, password.

14.PROTEZIONE DEI DATI NELLE COMUNICAZIONI

Il pericolo di perdere il controllo dei dati aumenta notevolmente in occasione del loro invio verso l'esterno. Ad esempio quando si invia una email, i dati in essa contenuti devono transitare attraverso più di un sistema informatico intermedio esterno rispetto a quello aziendale. Durante questi passaggi il contenuto può essere intercettato. Per questa ragione è preferibile utilizzare sistemi per la protezione dei dati tramite crittografia oppure tramite servizi di terze parti (come il caricamento su cloud o hosting di comprovata sicurezza).

15.CRITTOGRAFIA

Crittografare i dati significa sfruttare un sistema in grado di trasformarli, rendendoli privi di qualsiasi significato, consentendo di estrarne il contenuto originale solo a chi sia in possesso delle necessarie autorizzazioni. Dal punto di vista della sicurezza nelle comunicazioni, questo è equivalente ad inviare i dati in questione dopo averli racchiusi in un pacchetto al quale non è possibile accedere.

16.CRITTOGRAFIA E-EMAIL

Se l'azienda è provvista di un sistema per la protezione delle mail integrato nel proprio sistema informatico, per proteggere le comunicazioni con l'esterno sarà sufficiente utilizzare solo questo sistema per l'invio e la ricezione di dati. In alcuni casi, il sistema in questione prevede la generazione di codici di sicurezza che però devono essere inviati al destinatario utilizzando un altro sistema di comunicazione. Si crea in questo modo un secondo controllo che rende molto difficile l'intercettazione dei dati ad una persona non autorizzata. In alternativa, possono essere utilizzati software che permettono di crittografare singoli documenti o anche interi archivi. Anche in questo caso al destinatario dovrà essere comunicato un codice di accesso attraverso un secondo canale di comunicazione, per consentirgli di estrarre i contenuti dal messaggio inviato tramite email. In grado di protezione offerto può variare in modo significativo a seconda del software utilizzato.

17.SISTEMI CLOUD E HOSTING

L'alternativa più utilizzata all'invio tramite email è il caricamento su sistemi cloud o hosting affidabili oppure sotto il diretto controllo dell'azienda. In questo caso, al destinatario viene generalmente inviato un indirizzo internet al quale collegarsi per scaricare il materiale proveniente dal mittente. La protezione in questo caso può essere data da:

- Accesso al materiale caricato consentito solo a seguito di autenticazione di un profilo affidabile;
- Citazione del materiale invio della relativa chiave di decrittazione;
- Invio di codici/credenziali di accesso tramite canale indipendente.

Qualunque sia la strategia scelta per l'invio di dati tra quelle precedenti rimane fondamentale verificare con attenzione il destinatario e la sua identità prima di effettuare il trasferimento o comunicare dati di accesso.

18.PASSWORD

La scelta della password ha un'importanza straordinaria per garantire una efficace sicurezza dei dati. Spesso le regole per la scelta sono impostate dall'azienda, ma è in ogni caso utile conoscere le regole fondamentali che consentono di impostare una password che abbia due caratteristiche:

- Ogni password deve essere robusta;
- Ogni password deve essere facile da ricordare.

Per raggiungere il primo obiettivo, la password deve essere lunga. La tipologia di attacco alla password più semplice è infatti quello che viene definito brute force. Il metodo è banale: utilizzando un software, viene proposto al sistema di controllo accesso ogni possibile password, anche miliardi di volte al secondo, cambiando di volta in volta la composizione della stringa di caratteri che la compongono. Una password breve, soprattutto se di composizione semplice, può essere individuata in questo modo anche in meno di un secondo.il secondo requisito fondamentale è la complessità. Una buona password contiene caratteri appartenenti a diverse tipologie ovvero include:

- Lettere maiuscole;
- Lettere minuscole;
- Numeri;
- Caratteri speciali.

La complessità viene aumentata se questi vengono inseriti all'interno della stringa di caratteri e non all'inizio o alla fine. Occorre poi evitare che la password sia una parola di senso compiuto, anche se leggermente alterata. Un'altra forma di attacco più sofisticata prevede di tentare combinazioni casuali di caratteri, il sistema propone di volta in volta parole estratte da un dizionario, tentando di impiegarne anche le varianti più probabili. Rientrando tra le varianti più utilizzate: sostituire una lettera con un numero ad essa somigliante, plurali/singolari, uso di parole composte. Evitare i riferimenti alla propria persona o a chi ci è vicino. L'individuazione di una password può semplificarsi di molto se al suo interno inseriamo il nome del compagno, di un animale domestico, la nostra data di nascita o quella di nostro figlio, perché in tal caso qualcuno che ci conosca, o reperisca informazioni che ci riguardano in altro modo, potrebbe disporre di un pezzo della nostra password. Il numero di tentativi per individuarne il resto si ridurrà di molto, rendendo l'intera stringa più vulnerabile. Non utilizzare la stessa password per più account, servizi o dispositivi. Qualora un eventuale fuga di dati ai danni di un servizio utilizzato portasse ad una scoperta o diffusione, l'autore dell'attacco potrebbe ottenere l'accesso a dati che ci riguardano. Nella peggiore delle ipotesi un malintenzionato potrebbe accedere ai nostri sistemi di comunicazione, individuare nostri dati sensibili, ottenere accesso ai nostri dati di pagamento fino anche a riuscire a intrufolarsi nel sistema informatico aziendale. Una password deve essere facile da memorizzare, ma complessa da indovinare per un computer. Una stringa di otto caratteri completamente casuali può risultare più facile da scoprire di quanto non sia memorizzarla, dunque è meglio optare per un approccio più umano.se la password è troppo complicata si rischia di incappare in uno degli errori più gravi in assoluto: tenerne nota su foglietti o, peggio ancora, salvarli sul nostro dispositivo senza utilizzare un servizio di sicurezza.

19.CATTIVI ESEMPI

Secondo studi effettuati da specialisti del settore, facendo riferimento a password trafugate e pubblicate in rete, emerge che tra le 10 password più usate negli ultimi anni ci sono stabilmente:

123456

123456789

Abc123

Password

12345678

111111

123123

12345

1234567890

20.AUTENTICAZIONE IN DUE PASSAGGI

Quando possibile, meglio ricorrere a servizi che consentono di eseguire l'accesso in due passaggi, ad esempio:

- Inviando un codice di accesso temporaneo tramite un sms;
- Inviando un codice di accesso temporaneo tramite email;
- Chiedendo di inserire due password diverse tra loro.

In questo modo per un eventuale malintenzionato viene aggiunto un secondo ostacolo da superare, legato alla disponibilità di un dispositivo o di un'altra credenziale di accesso.

21.BUONE ABITUDINI PER LA GESTIONE SICURA DEI DISPOSITIVI

Le regole generali per un buon controllo degli accessi ai dati aziendali si applicano anche ai singoli dispositivi. Per la loro applicazione è pero necessario un contributo consapevole e positivo da parte del singolo utente del dispositivo, che dovrà rispettare poche semplici regole:

- Prestare attenzione alle periferiche impiegate;
- Proteggere l'accesso al dispositivo;
- Evitare la condivisione delle proprie credenziali;
- Non installare/eseguire programmi sconosciuti o non autorizzati dall'azienda.

L'uso di periferiche rimovibili come chiavette USB o hard disk portabili, può rappresentare un serio rischio per la sicurezza dei dati e dei sistemi informatici. E' infatti possibile configurare o modificare questi dispositivi perché non appena collegati ad un dispositivo siano in grado di avviare software dannoso oppure siano in grado di danneggiare irreparabilmente lo stesso dispositivo cui sono collegati. Per questi motivi è indispensabile diffidare, in generale, sia di dispositivi di origine non chiara che di dispositivi utilizzati con computer o altri sistemi della cui sicurezza non abbiamo certezze. Alcuni programmi malevoli sono infatti in grado di replicarsi autonomamente, senza fornire segnali evidenti, a bordo di dispositivi rimovibili per poi proseguire la catena di trasmissione. Si tratta di minacce concrete, in quanto in questo modo è possibile superare agilmente tutte le barriere realizzate tra dispositivi aziendali e reti esterne, sfruttando un inconsapevole complice interno. I software antivirus sono generalmente in grado di riconoscere e bloccare queste minacce ma, in assenza di maggiori garanzie, è preferibile evitare l'utilizzo di dispositivi rimovibili non forniti dall'azienda. Non dimentichiamo infine che un attacco può puntare anche "solo" alla distruzione dei dati o addirittura di un dispositivo. Esistono rischi anche in tal senso, sotto forma di dispositivi realizzati con l'esplicito scopo di apparire innocui e provocare danni irreparabili all'hardware del computer, tablet o smartphone cui vengono collegati, con il potenziale di comprometterne i supporti di memoria e dunque i documenti conservati localmente.

22.PROTEZIONE DELL'ACCESSO AL DISPOSITIVO

L'importanza di impedire l'accesso al proprio dispositivo quando questo è incustodito è fondamentale, e si realizza:

- Dotando il dispositivo stesso di un sistema di blocco, pin, password, ecc.;
- Bloccando il dispositivo ogni qualvolta ce ne allontaniamo.

Il blocco automatico dopo un certo numero di minuti, sebbene indispensabile, non sempre è sufficiente. Immaginiamo di assentarci per qualche minuto: durante la nostra assenza il dispositivo, così come ogni altro accesso da noi già eseguito, potrebbe rimanere a completa disposizione di un malintenzionato. In tema di dispositivi mobili utilizzati per gestire dati aziendali, è importante conoscere esistenza ed importanza delle funzionalità antifurto integrate nella maggior parte dei sistemi operativi più moderni (per smartphone, tablet e pc). Questi sistemi, una volta attivati e correttamente configurati, permettono in caso di smarrimento o furto del dispositivo di rintracciarlo e/o bloccarne l'accesso da remoto, in modo tale da rendere impossibile ottenerne qualsiasi dato da parte di chi ne fosse eventualmente entrato in possesso.

23.DISPOSITIVO DI MEMORIA PORTABILI

Nel caso si rendesse indispensabile impiegare un dispositivo di memoria portatile (chiavetta usb, hard disk esterni, supporti ottici), oltre alla necessità di ricorrere a dispositivi affidabili sarà necessario preoccuparsi dell'eventuale smarrimento o sottrazione del dispositivo. La soluzione a questo problema è ancora una volta quella di non trasportare mai dati che necessitino di particolare protezione in forma facilmente accessibile, bensì di sfruttare un sistema per la loro crittazione/decrittazione locale. Una volta scelta una password sufficientemente sicura, anche la protezione di un semplice archivio compresso può essere sufficiente a far desistere chi ne entrasse in possesso. Condividendo le proprie credenziali di accesso a un dispositivo, anche se per finalità legittime, si concretizza uno scenario di aumento del rischio di per la sicurezza. Questo è in parte dovuto al supporto utilizzato per trasmettere tale credenziali, in parte l'impossibilità di conoscere completamente le intenzioni del destinatario.

24.INSTALLAZIONE E USO DI SOFTWARE NON AFFIDABILI

È buona norma verificare attentamente origine e affidabilità di qualsiasi applicazione o software prima di installarli e/o utilizzarli, in particolar modo quando l'operazione viene eseguita con un dispositivo impiegato anche per gestire dati legati al lavoro. Alcuni produttori di software possono infatti nascondere ed installare o eseguire, accanto al programma desiderato e in apparenza innocuo, processi e altri software che possono portare a una grave compromissione della sicurezza. Per questi motivi spesso l'installazione di programmi viene impedita all'utenti di un dispositivo consentendola solo a membri dell'ufficio tecnico aziendale.

25.SMALTIMENTO RIFIUTI

La protezione di un dispositivo e dei dati aziendali contro il cybercrime non interessa la sola vita utile. Prima di avviare un vecchio dispositivo verso lo smaltimento, è bene effettuare una cancellazione sicura, ricorrendo alle funzionalità del sistema operativo o utilizzare software dedicati in grado di cancellare i dati in esso contenuti rendendoli completamente irrecuperabili. Qualora compatibile con il grado di dispositivo, e con i dati in esso contenuti, può essere considerata anche l'operazione di distruggere fisicamente i supporti di memoria, deformandoli o danneggiandoli in modo tale da rendere fisicamente impossibile il loro recupero.

26.PHISHING: CARATTERISTICHE E PROTEZIONE

Con l'avanzare degli strumenti tecnologici per la prevenzione e la protezione dagli attacchi, tecniche per l'accesso forzato ai sistemi informatici hanno sempre più lasciato spazio a metodologie passate sul cosiddetto social engineering. Una volta raggiunto un certo livello di protezione l'anello debole della catena cybersecurity diventa l'utente stesso del sistema. Il social engineering sposta l'attenzione di chi attacca verso

quest'ultimo, cercando di sfruttarne curiosità, reazioni emotive o anche solo la distrazione, al fine di spingere le persone a rivelare determinate informazioni o consentire l'accesso a un sistema informatico. Tra le metodologie cybercrime che si sono sviluppate sfruttando questi principi sì è quella del phishing ovvero la tecnica con cui il malintenzionato utilizza varie tecniche per far abboccare la sua vittima e ottenerne la cooperazione nell'invio di informazioni e dati sensibili (credenziali di accesso, dati di pagamento, ecc.) O scaricamento/esecuzione di programmi malevoli o virus. Il mezzo di contatto iniziale privilegiato per questi tentativi di attacchi e l'invio di e-mail spam, realizzate con cura e ti inviate tramite i metodi che consentono di far somigliare i messaggi a documenti autentici e legittimi. Il malintenzionato può clonare il formato dell'e-mail solitamente inviate da istituti di credito, oppure simulare nella forma e nel contenuto un messaggio e-mail confidenziale inviato da parte di un possibile cliente, oppure ancora puntare sull'avidità del bersaglio, promettendo facce dei guadagni o l'incasso di somme di denaro. L'obiettivo è in ogni caso catturare l'attenzione del ricevente con messaggi che riescano a distrare dagli elementi sospetti e invogliano a seguire l'azione desiderata. Spesso l'email richiede, trasmettendo un senso di urgenza e con il pretesto di verificare i nostri dati o di richiedere una nostra azione per evitare perdite economiche o altre sanzioni, di cliccare su un collegamento internet. Il collegamento in questione porta la vittima verso un portale realizzato in tutto e per tutto come clone del portale legittimo dell'ente cui si è ispirato il cybercriminale, dove viene richiesto all'utente l'inserimento dei propri dati personali. Una volta inseriti ed inviati, i dati vengono memorizzati dall'organizzatore del raggiro, mentre la vittima viene restituita una pagina di errore o di ringraziamento ufficiale per aver verificato i propri dati. Altre varianti possono richiedere, sempre simulando il messaggio inizio ufficiale di un'importante azienda o banca oppure simulando una email confidenziale (anche "clonando " l'indirizzo email di un nostro cliente o conoscente), di scaricare un documento o altro file allegato all'email. In questi casi può essere lo stesso documento, anche se in apparenza innocuo, a completare l'attacco, installando o avviando direttamente programmi malevoli. Le varianti più sofisticate, che invece sono direttamente indirizzate verso uno specifico bersaglio e cercano di instaurare una conversazione in apparenza ordinaria con la vittima, al fine di ottenerne la fiducia e procedere solo in un secondo momento con i restanti passi.

Protezione dal phishing:

- Controllare l'indirizzo del mittente
- Diffidare di messaggi contenenti formule generiche o prive di informazioni di contatto del mittente;
- Diffidare di collegamenti internet accorciati, contesto a video non corrispondente alla reale destinazione, o indirizzo di destinazione contraffatto
- Diffidare di messaggi sgrammaticati e malformattati
- Evitare di scaricare allegati non richiesti.

Molti browser internet dispongono di sistemi integrati che bloccano l'accesso a siti riconosciuti come pericolosi perché utilizzati a scopo di truffa/phishing. Un ulteriore indizio di sicurezza di un sito internet e' la presenza di una chiave di sicurezza verificata: se nella barra degli indirizzi del sistema di navigazione usato notiamo un piccolo lucchetto il sito in questione sta proteggendo le informazioni scambiate da e verso il nostro dispositivo.