Misure di sicurezza da adottare nell'ente locale

A domanda risponde Prof. Avv. Michele IASELLI

2 luglio 2024 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

Cosa si intende per cyber risk?

La rivoluzione digitale sta portando molti benefici alla nostra società, ma, come spesso accade, bisogna considerare anche il rovescio della medaglia. Difatti, accanto agli innumerevoli benefici, l'uso incontrollato di Internet può comportare una quantità notevole di insidie e problematiche che rientrano nell'ambito di quel fenomeno definito cyber risk "rischio informatico (o ICT)".

Il rischio informatico può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

In particolare questi ultimi possono essere:
- danneggiamento di hardware e software;
- errori nell’esecuzione delle operazioni nei sistemi;
- malfunzionamento dei sistemi;
- programmi indesiderati.

Tali rischi possono verificarsi in diversi casi:

1. i programmi “virus” destinati ad alterare od impedire il funzionamento dei sistemi informatici;
2. le truffe informatiche;
3. l’accesso abusivo a sistemi informatici o telematici;
4. il cyberstalking;
5. il cyberbullismo;
6. la pedo-pornografia;
7. il revenge porn.

Solo una piena consapevolezza del concetto di sicurezza informatica può davvero metterci al riparo da sgradevoli sorprese.

Ogni giorno vengono compiuti migliaia di attacchi informatici attraverso le tecniche più varie e termini come malware, ransomware, trojan horse, account cracking, phishing, sono diventati parte del vocabolario anche per i non esperti.

J. Edgar Hoover, capo dell'FBI (Federal Bureau of Investigation) moltissimi anni fa affermava: "*L'unico computer a prova di hacker è quello spento, non collegato ad Internet e chiuso a chiave in una cassaforte*". Appena viene riacceso diventa potenzialmente vulnerabile e può essere attaccato, ad esempio durante l'installazione di eventuali aggiornamenti al sistema operativo.

Naturalmente per evitare attacchi informatici, o almeno per limitarne le conseguenze, è necessario adottare delle contromisure; i calcolatori e le reti di telecomunicazione necessitano di protezione anche se come in qualsiasi ambiente la sicurezza assoluta non è concretamente realizzabile.
Il modo per proteggersi è imparare a riconoscere le origini del rischio. Gli strumenti di difesa informatica sono molteplici, si pensi antivirus, antispyware, blocco popup, firewall ecc., ma tuttavia non sempre si rivelano efficienti, in quanto esistono codici malevoli in grado di aggirare facilmente le difese, anche con l'inconsapevole complicità degli stessi utenti.

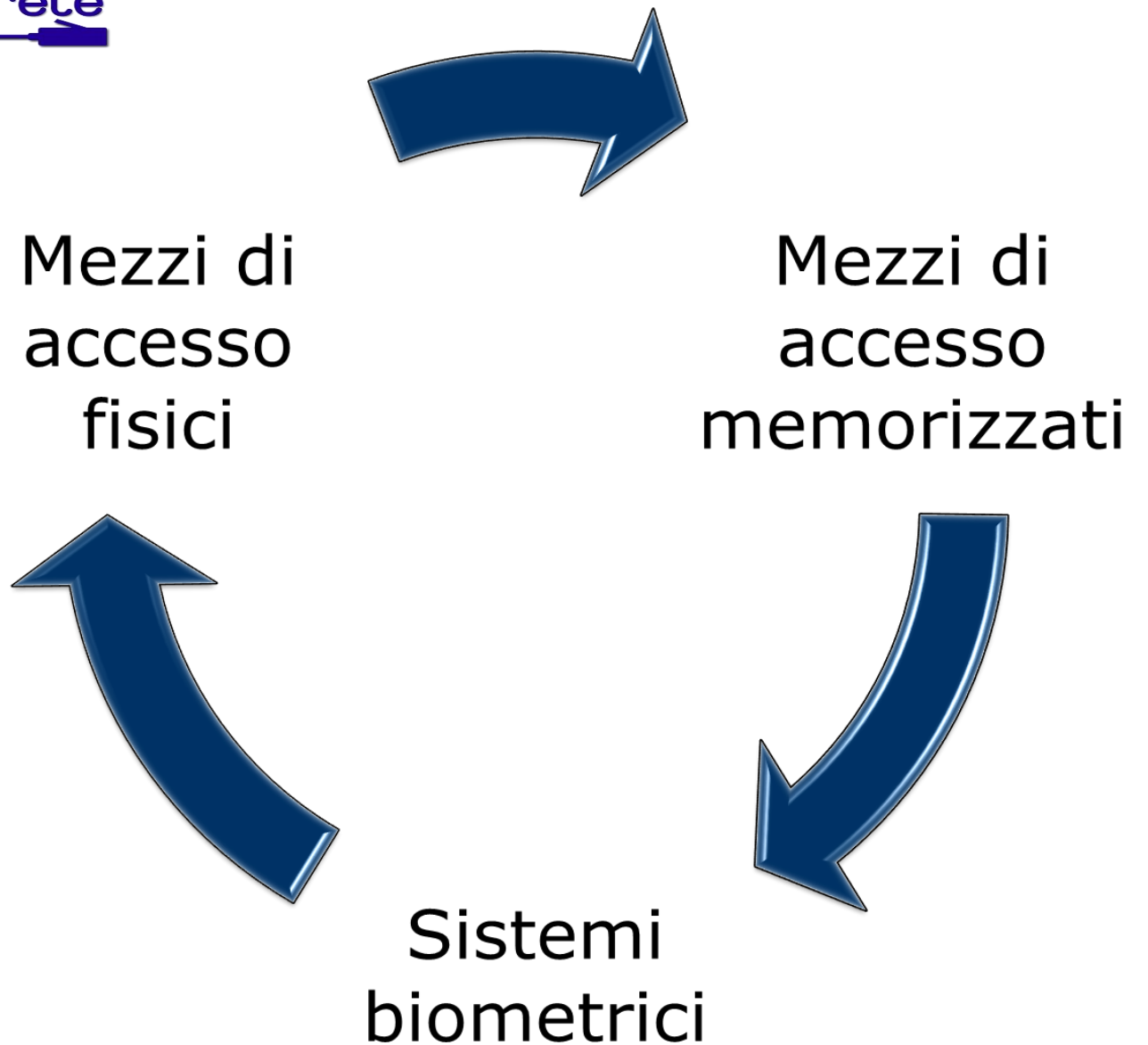
La sicurezza informatica

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.
Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e la elaborazione a distanza (informatica distribuita).

Riguardo l’aspetto “sicurezza” connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati.

Come può essere garantita la sicurezza?


Mezzi di accesso fisici
Mezzi di accesso memorizzati
Sistemi biometrici

La sicurezza nel GDPR

Non poteva, ovviamente, mancare nel Regolamento UE n. 2016/679 sulla protezione dei dati personali un chiaro riferimento alle misure di sicurezza che già vengono menzionate nell'art. 24 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

Più nello specifico, l’art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento.
Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Tali misure comprendono:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel recente passato si è assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi:
Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati.
Il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.

La combinazione di questi due fattori fa sì che misure tecniche adeguate, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attività degli utenti rimangano sempre all'interno dei limiti previsti.
Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Naturalmente le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli **inventari dei dispositivi e dei software**, che costituiscono le prime due classi di misure, nonché la **protezione della configurazione** (di hardware e software), che è quella immediatamente successiva.

La quarta classe deve la sua priorità alla duplice rilevanza **dell'analisi delle vulnerabilità**.
In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace.
Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe è rivolta alla gestione degli utenti, in particolare con riferimento **all'attività degli amministratori** ed ad un uso appropriato dei relativi privilegi.

La sesta classe rappresentata dalle **difese contro i malware** deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.

Le **copie di sicurezza**, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.
L'ultima classe, la **Protezione dei Dati**, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

I cybercrimes

Dare una definizione di crimine informatico meglio noto come cybercrime, non è semplice poiché tale termine include al proprio interno diverse condotte illecite, di varia natura, aventi come denominatore comune l'utilizzo di un computer o di un dispositivo informatico.

In genere per crimine informatico si intende un qualunque comportamento criminoso, nel quale il computer è coinvolto come mezzo o come oggetto dell'azione delittuosa, ma in tale categoria rientrano anche quegli illeciti in cui il computer si interpone tra l'autore del crimine e la vittima o comunque rappresenta lo strumento principale per compiere una determinata azione criminosa.

E’ possibile, inoltre, distinguere tra reati eventualmente e necessariamente informatici.

- I primi sono quei reati in cui le tecnologie informatiche hanno solo ampliato le modalità di realizzazione di un reato già esistente, un esempio può essere rappresentato dal furto o dall’appropriazione indebita di fondi realizzati utilizzando le tecnologie informatiche.
- I reati necessariamente informatici invece, sono quelli che hanno comportato la nascita di figure criminose completamente nuove, un esempio è dato dal delitto di accesso abusivo ad un sistema informatico o telematico (art 615-ter codice penale).

Caratteristiche dei crimini informatici

Secondo un’attenta ricerca i cybercrimini si differenziano dai crimini tradizionali in quanto:

a) sono tecnicamente più semplici da commettere in quanto non richiedono particolari conoscenze informatiche

b) non richiedono un investimento criminale iniziale ingente, considerando il profitto che da essi può derivare;

c) possono essere commessi in ogni parte del mondo, in quanto non è richiesta la presenza fisica al momento della consumazione del fatto;

d) su di essi non sempre v’è chiarezza ed uniformità normativa a livello europeo ed internazionale.

La situazione normativa in Italia

I reati informatici sono notevolmente cresciuti di numero negli ultimi tempi, in parallelo con la diffusione dell'informatica e della telematica in ogni settore della vita sociale.

Di conseguenza, si è reso necessario l'intervento frequente e settoriale del legislatore per la lacunosità della normativa precedente che concerneva "fatti illeciti" ben lontani, sia dal punto di vista della individuazione del bene giuridico protetto, sia sotto il profilo della condotta e dell'oggetto "materiale" del reato, dai c.d. computer crimes generati dall'evoluzione della tecnologia informatica.

I reati informatici nel Codice Penale

Leggi

- Legge 547/93
- Legge 48/2008

Principali norme del codice

Art. 615-ter Accesso abusivo ad un sistema informatico o telematico
Art. 615-quinquies Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
Art. 635 - bis Danneggiamento di sistemi informatici o telematici
Art. 640-ter Frode informatica

Gli attacchi provenienti dal web

Quando si parla di attacchi provenienti dal Web non si può fare a meno di pensare ai virus, ma vedremo che non sono gli unici pericoli e tra l'altro non sono tutti uguali.

Un *virus informatico* è composto da un insieme di istruzioni da pochi byte ad alcuni kilobyte (per rendere più difficile da individuare e facile da copiare), tende ad eseguire soltanto poche operazioni ed impiega il minor numero di risorse, in modo da rendersi il più possibile invisibile.

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:
1. ricercare i file adatti ad essere infettati controllando che non contengano già una copia, per evitare una ripetuta infezione dello stesso file;
2. copiare il codice virale all'interno di ogni file selezionato perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

Ma quando sentiamo parlare di virus, in genere ricomprendiamo malware, trojan horse, worm mettendoli tutto sullo stesso piano sia per genesi che per effetti, invece, è necessario fare delle precisazioni in quanto esistono delle sostanziali differenze tra queste diverse tipologie di virus.
In primo luogo c'è da precisare che sia i virus, sia i trojan horse che i worm rientrano nella categoria più generale dei malware.

Il termine malware deriva dalla contrazione di due termini inglesi, rispettivamente “MALicious” e “softWARE”, e viene utilizzato per indicare tutti quei programmi realizzati per danneggiare le macchine che li eseguono, da qui il nome di software malevolo. I programmi malware se riescono ad entrare in un computer possono creare dei veri e propri danni impedendone il corretto funzionamento, oppure possono spiare tutto quello che scriviamo, sottrarre dati sensibili, come ad esempio i numeri della carta di credito, per trasmetterli poi ad altri malintenzionati.

Il *Trojan horse*, letteralmente cavallo di Troia (chiaro riferimento all'inganno della mitologia omerica), può essere definito come un "programma apparentemente utile, ma che contiene funzioni nascoste atte ad abusare dei privilegi dell'utente che lo esegue".
A differenza dei virus non ha la capacità di autoriproduzione e diffusione, ma è l'utente a scaricarlo. Di solito si presenta sotto forma di gioco, screensaver ed altri articoli di interesse, ma una volta eseguito, il trojan installa segretamente il file server sul computer della vittima, compiendo allo stesso tempo tutte le operazioni di "copertura" che si suppone debba compiere.

I *Worm* sono programmi software dannosi sviluppati per diffondersi il più rapidamente possibile dopo che il PC è stato infettato. A differenza dei comuni virus, non sfruttano la presenza di altri programmi per moltiplicarsi, ma sfruttano i dispositivi di memorizzazione come le chiavette USB, le e-mail o le vulnerabilità nel sistema operativo. La loro propagazione rallenta le prestazioni dei PC e delle reti, diffondono dati all'esterno e possono provocare problemi al funzionamento generale del PC.

Come ultima frontiera dei pericoli digitali non possono essere dimenticati i micidiali "*Ransomware*" programmi maligni che, utilizzando efficaci tecniche di cifratura dei file, rendono inutilizzabili documenti, archivi, immagini e qualunque altro contenuto venga memorizzato sul disco fisso. L'operazione criminale è il preludio di una manovra estorsiva che si realizza con il rilascio di una salvifica parola chiave a fronte del pagamento di una determinata somma: "ransom", infatti, è il termine anglofono che identifica il riscatto.

“Wannacry” ha creato non pochi danni nel settore pubblico, ma per il passato anche “cryptolocker” è stato l’incubo di molti utenti della rete.

Da Telecom Italia-TIM <1493615664clientiservizio@tim1493615664.it>

Oggetto **Fattura TIM linea Fissa - Maggio 2017 - scadenza 01/05/2017** 01/05/2017 07:14

IL FUTURO FIRMATO TELECOM ITALIA | TIM

Gentile cliente,

ti informiamo che la tua fattura TIM di**Maggio 2017** relativa alla linea **Fattura 00726377-288389** è stata appena emessa ed è disponibile online.

Si prega di scaricare il fattura attaccato

Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la **fattura TIM** esclusivamente online. **Risparmierai così le spese di spedizione postale**.

Ti aspettiamo presto su **www.tim.it**

Grazie

Servizio Clienti tim.it

1 allegato: Fattura 00726377-288389.zip dimensione sconosciuta

Come difendersi dai virus

1. La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.).
2. Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze. (Ad esempio non aprire mai allegati con estensioni "strane«: estensione ".exe" sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
3. non scaricare software da siti sospetti (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);
4. scaricare preferibilmente app e programmi da market ufficiali, i cui gestori effettuano controlli sui prodotti e dove è eventualmente possibile leggere i commenti di altri utenti che contengono avvisi sui potenziali rischi;

E' inoltre utile:

- installare su tutti i dispositivi un antivirus con estensioni anti-malware;
- mantenere costantemente aggiornati il sistema operativo oltre che i software e le app che vengono utilizzati più spesso;
- utilizzare dei sistemi di backup che salvino (anche in maniera automatica) una copia dei dati (sono disponibili soluzioni anche libere e gratuite per tutti i sistemi operativi). Con un corretto backup, in caso di necessità, si potranno così ripristinare i dati contenuti nel dispositivo, quantomeno fino all'ultimo salvataggio.

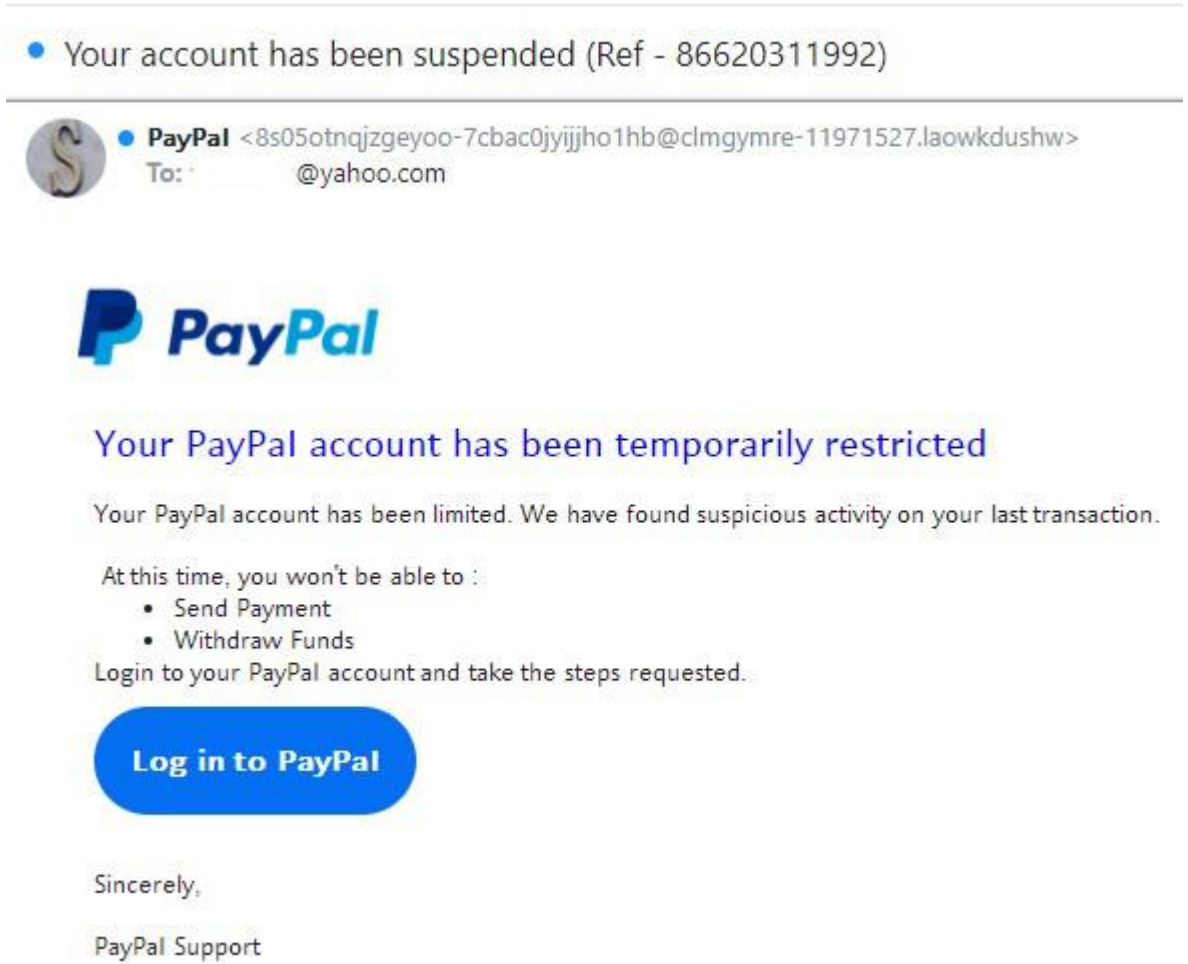
Le truffe informatiche più diffuse

Phishing

Il phishing è un tipo di frode ideato proprio allo scopo di rubare l'identità di un utente.
Quando viene attuato, una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti.
In concreto il phishing viene messo in atto da un utente malintenzionato che invia milioni di false e-mail che sembrano provenire da siti Web noti o fidati come il sito della propria banca o della società di emissione della carta di credito.

I messaggi di posta elettronica e i siti Web in cui l'utente viene spesso indirizzato per loro tramite sembrano sufficientemente ufficiali da trarre in inganno molte persone sulla loro autenticità. Ritenendo queste e-mail attendibili, gli utenti troppo spesso rispondono ingenuamente a richieste di numeri di carta di credito, password, informazioni su account ed altre informazioni personali.

Per far sembrare tali messaggi di posta elettronica ancora più veritieri, un esperto di contraffazione potrebbe inserirvi un collegamento che apparentemente consente di accedere ad un sito Web autentico, ma che di fatto conduce ad un sito contraffatto o persino una finestra a comparsa dall'aspetto identico al rispettivo sito ufficiale.



Your account has been suspended (Ref - 86620311992)

PayPal <8s05otnqjzgeyoo-7cbac0jyijjho1hb@clmgymre-11971527.laowkdushw>
To: @yahoo.com

PayPal

Your PayPal account has been temporarily restricted

Your PayPal account has been limited. We have found suspicious activity on your last transaction.

At this time, you won't be able to :

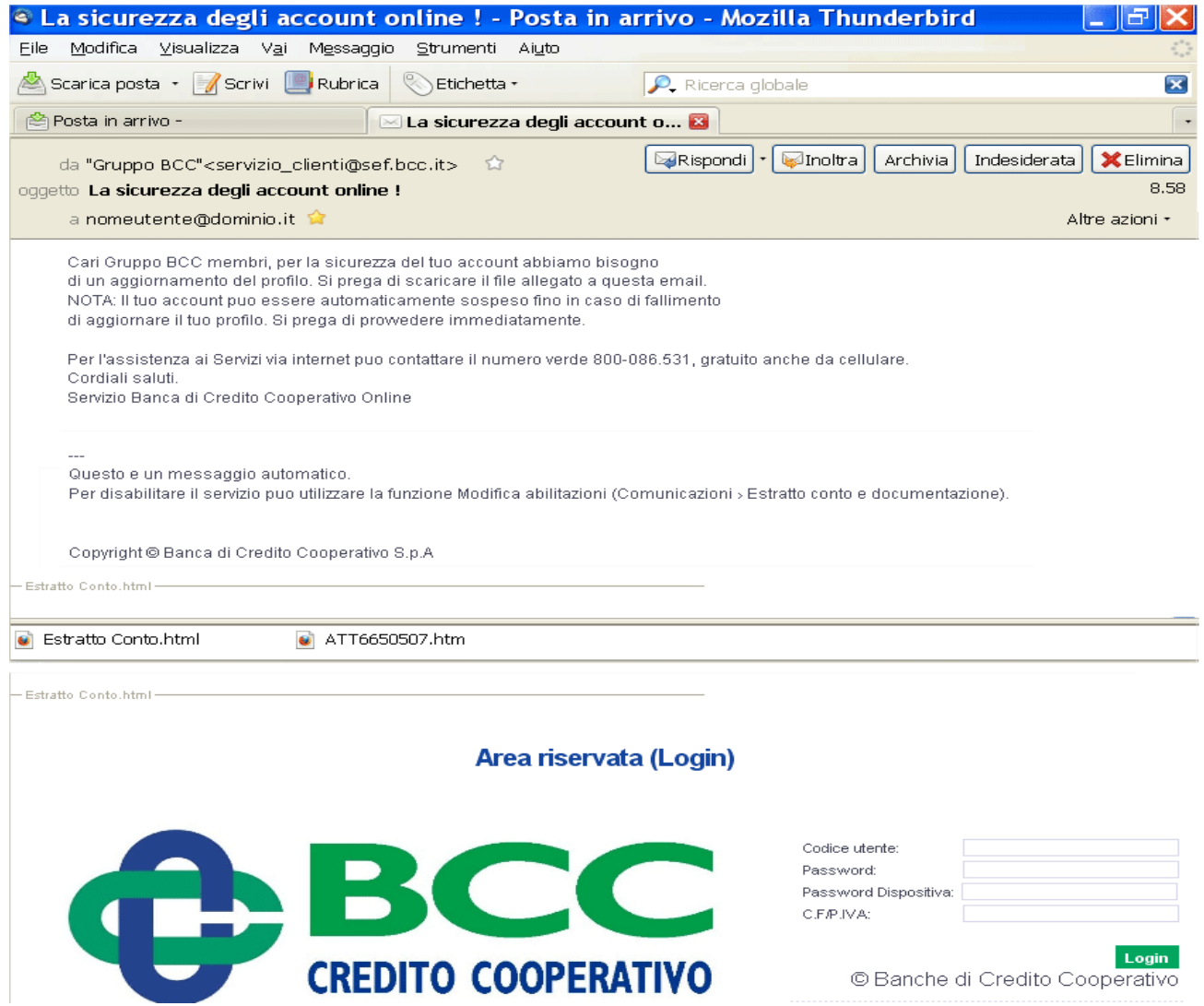
- Send Payment
- Withdraw Funds

Login to your PayPal account and take the steps requested.

Log in to PayPal

Sincerely,

PayPal Support


La sicurezza degli account online ! - Posta in arrivo - Mozilla Thunderbird
File Modifica Visualizza Vai Messaggio Strumenti Aiuto
Scarica posta Scrivi Rubrica Etichetta Ricerca globale
Posta in arrivo - La sicurezza degli account o...
da "Gruppo BCC"<servizio_clienti@sef.bcc.it>
oggetto La sicurezza degli account online !
a nomeutente@dominio.it
Rispondi Inoltra Archivia Indesiderata Elimina
8.58
Altre azioni
Cari Gruppo BCC membri, per la sicurezza del tuo account abbiamo bisogno
di un aggiornamento del profilo. Si prega di scaricare il file allegato a questa email.
NOTA: Il tuo account puo essere automaticamente sospeso fino in caso di fallimento
di aggiornare il tuo profilo. Si prega di prowedere immediatamente.
Per l'assistenza ai Servizi via internet puo contattare il numero verde 800-086.531, gratuito anche da cellulare.
Cordiali saluti.
Servizio Banca di Credito Cooperativo Online

Questo e un messaggio automatico.
Per disabilitare il servizio puo utilizzare la funzione Modifica abilitazioni (Comunicazioni › Estratto conto e documentazione).
Copyright © Banca di Credito Cooperativo S.p.A
Estratto Conto.html
Estratto Conto.html ATT6650507.htm
Estratto Conto.html
Area riservata (Login)
BCC
CREDITO COOPERATIVO
Codice utente:
Password:
Password Dispositiva:
C.F./P.IVA:
Login
© Banche di Credito Cooperativo

Spear phishing

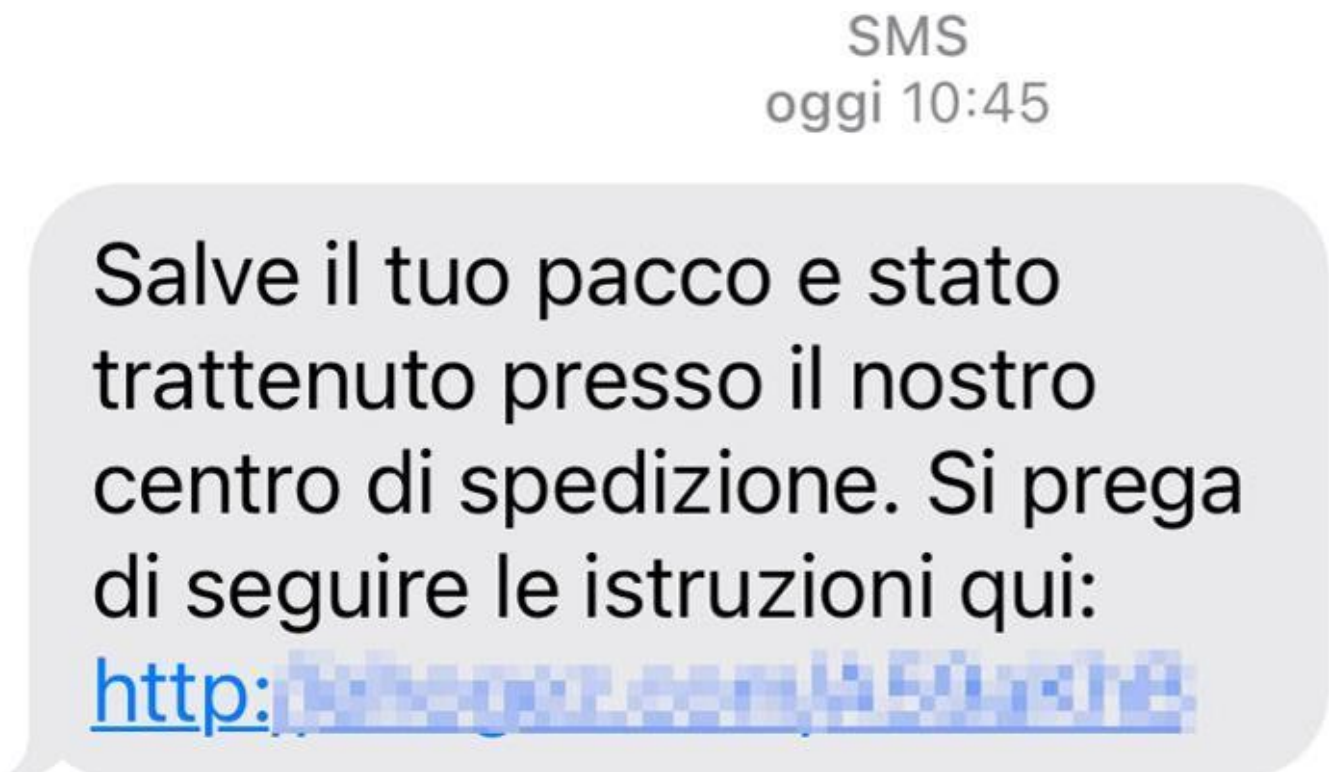
Con lo spear phishing, invece, la mail è indirizzata a una persona, un'organizzazione o un'azienda specifica. Sebbene abbia naturalmente l'obiettivo di sottrarre dati per scopi dannosi, i cybercriminali potrebbero anche voler installare malware sul computer dell'utente preso di mira.

Smishing

Lo Smishing (o phishing tramite SMS) è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti (ad esempio, per poi sottrarre denaro da conti e carte di credito).
I messaggi di smishing invitano i destinatari a compiere azioni (cliccare link, ecc.) o fornire informazioni con urgenza, per non rischiare danni (es: blocco di utenze, blocco della carta di credito o del conto) o sanzioni.


Gentile Cliente, un nuovo dispositivo, risulta connesso al suo conto, se non sei tu, verifica ora: https://verifica-appn26-online.preview-domain.com


BNL
giovedì Oggi
Gentile cliente, il suo conto è momentaneamente sospeso per motivi di sicurezza.Lo attivi al seguente link: bit.ly/BNL-IT Distinti Saluti BNL Gruppo BNP Paribas


SMS
oggi 10:45
Salve il tuo pacco e stato trattenuto presso il nostro centro di spedizione. Si prega di seguire le istruzioni qui:
http:

Vishing

Il vishing (o phishing vocale) è una forma di truffa, sempre più diffusa, che utilizza il telefono come strumento per appropriarsi di dati personali - specie di natura bancaria o legati alle carte di credito - e sottrarre poi somme di denaro più o meno ingenti.
Di solito le vittime vengono contattate telefonicamente da finti operatori (di banche o di società che gestiscono bancomat o carte di credito) i quali, con la scusa di presunte “anomalie”, chiedono alle persone, nel loro stesso interesse, di collaborare a mettere in campo necessarie (e false) “procedure di sicurezza”.

Nel caso più frequente, i truffatori (i “visher”) chiedono direttamente di fornire i riferimenti del conto corrente o della carta di credito (come il PIN del bancomat o quello utilizzato per l’Internet banking, il numero della carta, il codice di sicurezza sul retro della carta, i dati dell’OTP cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.).

Come difendersi da queste truffe?

1. Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti.
2. E’ bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e- mail, sms, social media o chat.
3. Se si ricevono messaggi sospetti, è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere virus o programmi trojan horse capaci di prendere il controllo di pc e smartphone.
4. Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.
5. Capita spesso che i messaggi di phishing contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.
6. Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente.
7. Se si fanno acquisti online, è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.
8. Per proteggere conti bancari e carte di credito è bene controllare spesso le movimentazioni e attivare sistemi di *alert* automatico che avvisano l’utente di ogni operazione effettuata.
9. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile contattare direttamente la banca o il gestore della carta di credito attraverso canali di comunicazione conosciuti e affidabili.

La predisposizione del Regolamento Informatico

CAPO I – I PRINCIPI

ART. 1 - INTRODUZIONE, DEFINIZIONI E FINALITA'
ART. 2 - AMBITO DI APPLICAZIONE
ART. 3 - TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE
ART. 4 - RESPONSABILITA' PERSONALE DELL'UTENTE
ART. 5 - I CONTROLLI
- I principi
- I controlli non autorizzati

CAPO II – MISURE TECNICHE ED ORGANIZZATIVE

ART. 6 - AMMINISTRATORI DEL SISTEMA
ART. 7 - ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD
ART. 8 - POSTAZIONI DI LAVORO

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

ART. 9 - PERSONAL COMPUTER E COMPUTER PORTATILI
ART. 10 - SOFTWARE
ART. 11 - DISPOSITIVI MOBILI DI CONNESSIONE (INTERNET KEY)
ART. 12 - DISPOSITIVI DI MEMORIA PORTATILI
ART. 13 - STAMPANTI, FOTOCOPIATRICI E FAX
ART. 14 - STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

ART. 15 - GESTIONE E UTILIZZO DELLA RETE INTERNET
ART. 16 - GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

CAPO V – DISPOSIZIONI FINALI

ART. 17 - SANZIONI
ART. 18 - INFORMATIVA EX ART. 13 D.LGS. REG. UE n. 2016/679 AGLI UTENTI
ART. 19 - COMUNICAZIONI
ART. 20 - APPROVAZIONE DEL DISCIPLINARE