Sicurezza e Privacy

Tecnologie Informatiche
Istituti Tecnici - Classi Prime

Panoramica

- Sicurezza (Security)
- Minacce alla sicurezza
  - Minacce esterne
  - Minacce interne
- Privacy (Riservatezza)
- Minacce alla riservatezza
  - Minacce esterne
  - Minacce interne

Definizioni

Sicurezza: "Insieme di mezzi e tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni informatici" *(Wikipedia)*

Privacy: "Diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione" *(Garante privacy)*

Minacce alla Sicurezza

- Malware
  - Virus
  - Worm
  - Trojan
  - SpyWare e AdWare
  - RansomWare
- Social Engineering
- Phishing
- Pharming
- Vulnerabilità
- Hoax e SPAM
- Cookies
- Chat e IM
- Wireless LAN

MalWare

Definizione: si dice **MalWare** (***Mal****icious* *Soft****ware*** ossia "programma maligno") un software creato con lo scopo di causare danni piu o meno gravi a un sistema informatico su cui viene eseguito e ai dati degli utenti

MalWare

Vi sono vari tipi di MalWare, ciascuno con sue caratteristiche specifiche:

- Virus
- Worm
- Trojan
- SpyWare
- Keylogger
- AdWare
- RansomWare

Si distinguono per il modo che utilizzano per diffondersi

Si distinguono per l'obiettivo che hanno e quello che fanno

Virus

Un **Virus** è una sequenza di istruzioni inserita all'interno di un programma (il programma "infettato")

Di norma il virus è invisibile, in quanto il programma ospite funziona correttamente, mentre il virus opera in modo da non poter essere rilevato se non con strumenti appositi (antivirus)

Il virus si propaga inserendo copie di sé stesso dentro altri programmi, che diventano così veicoli per ulteriori infezioni

Virus

Oltre a replicarsi, il **Virus** può svolgere altre operazioni, più o meno dannose, quali:

- fare apparire messaggi (banner, popup)
- aprire *backdoor* per consentire ad altri l'accesso remoto al computer
- prelevare dati (da disco oppure da altri dispositivi quali ad es. microfono e webcam)
- modificare o cancellare dati
- attivare servizi a pagamento via SMS

Worm

Un **Worm**, diversamente dal Virus, è un programma vero e proprio

- Sfrutta lacune di sicurezza per eseguire operazioni di norma non consentite
- Si propaga attraverso la rete replicandosi da un computer all'altro

I rischi per la sicurezza sono più o meno gli stessi già visti per i Virus

Trojan

Un **Trojan** è un programma nascosto dentro applicazioni o dati utente (foto, documenti, brani audio o video)

I Trojan si diffondono:

- scaricando file infetti da Internet (p.es. copie pirata di software, film e musica protetti da copyright, ecc)
- ricevendo file infetti come allegati email (apparentemente innocui)

I rischi per la sicurezza sono più o meno gli stessi già visti per i Virus

SpyWare

Uno **SpyWare** è un programma che raccoglie all'insaputa dell'utente informazioni sulle sue abitudini di navigazione, credenziali di accesso, configurazioni di sistema, ecc per trasmetterle a un indirizzo predefinito.

Le informazioni raccolte possono essere usate per gli scopi più disparati, (spionaggio, ricatto, sostituzione di persona, stalking, ecc)

SpyWare - Keylogger

Un **Keylogger** è un particolare tipo di SpyWare che intercetta tutti i tasti premuti e quindi permette di scoprire le password digitate dall'utente

AdWare

Un **AdWare** è un programma che raccoglie all'insaputa dell'utente informazioni sulle sue abitudini di navigazione

Le informazioni raccolte vengono utilizzate a scopi pubblicitari

RansomWare

Un **RansomWare** è un particolare tipo di Virus (o Trojan) che codifica i dati presenti sull'hard disk e sui dischi di rete in modo da renderli inaccessibili a chi non possegga la chiave di decodifica

La chiave può essere ottenuta solo tramite pagamento di un riscatto (ransom)

Il pagamento però non garantisce che la chiave verrà realmente fornita ...

Alternative: recupero dati da backup o perdita definitiva dei dati

Wannacry screenshot

Wannacry (Wikipedia)

RansomWare


Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

Social Engineering

Le tecniche di **Social Engineering** sfruttano le vulnerabilità dell'elemento umano

Tipicamente sono utilizzate per attaccare grandi organizzazioni, facendo leva sugli anelli deboli della catena (p.es. ignari impiegati) per infiltrare Virus e Trojan o per far loro effettuare operazioni non autorizzate (p.es. bonifici bancari ...)

Vi sono anche attacchi mirati ad individui, sfruttandone le debolezze (p.es. truffe sentimentali)

Articolo su "La Stampa"

Tentativo di furto dati personali

Tentativo di ricatto

Phishing

Il **Phishing** è una forma di Social Engineering mirata a "pescare" la vittima attirandola in una trappola.

Consiste nell'invio di messaggi fraudolenti nei quali, fingendo che sia stato inviato da una banca, si chiede di confermare le proprie credenziali pena la decadenza del conto bancario in questione

Le credenziali vengono poi utilizzate per effettuare operazioni bancarie a spese della vittima

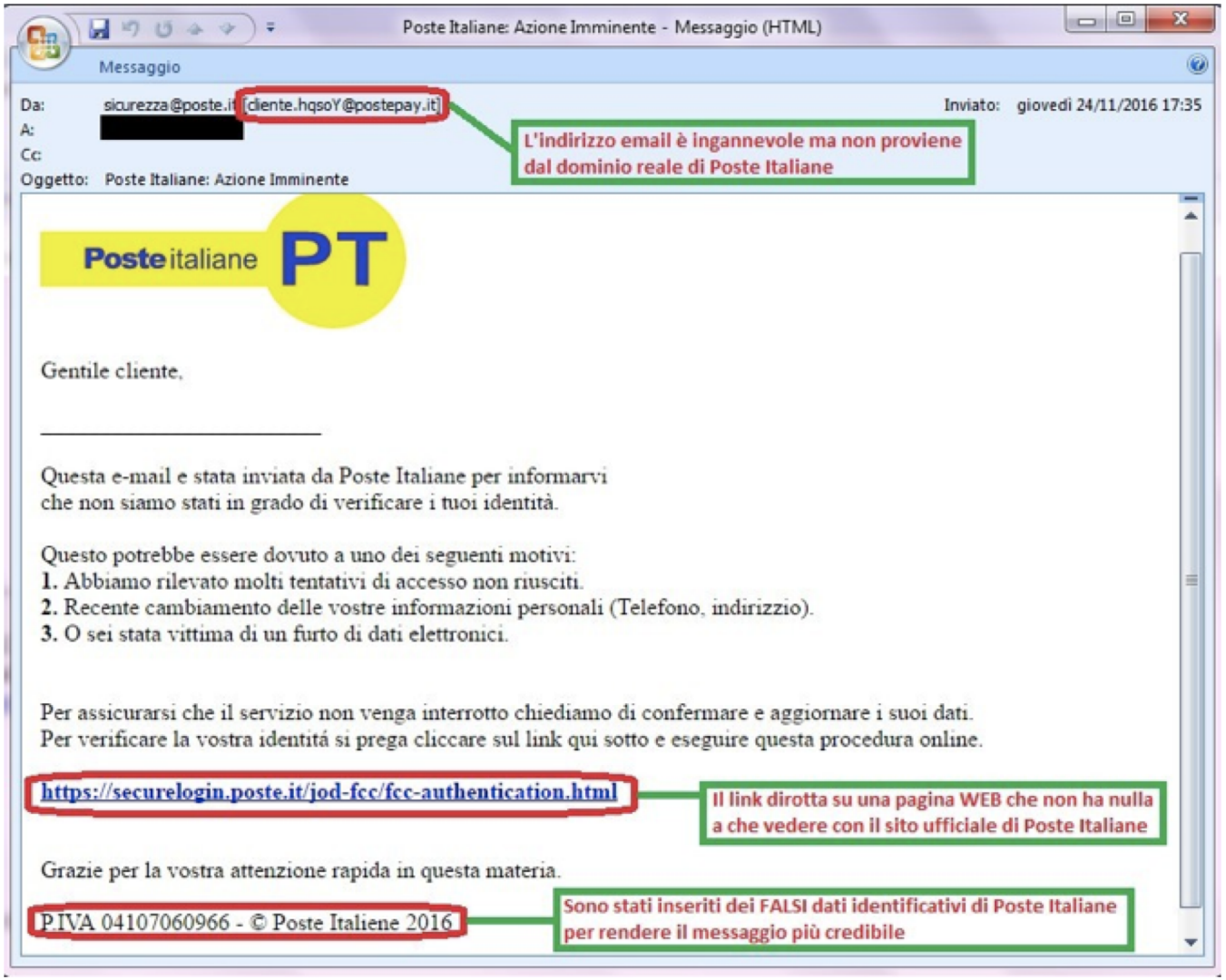
Pharming

Il **Pharming** è una tecnica simile al phishing, che fa si che, digitando l'indirizzo di un sito web lecito, si venga diretti verso un altro sito, identico a quello lecito, ma falso

Esempio: la visita ad un sito bancario fasullo nel quale l'ignaro utente immette le proprie credenziali (autentiche!)

Le credenziali vengono poi utilizzate dall'attaccante per accedere al sito vero ed effettuare operazioni bancarie a spese della vittima

Pharming e phishing: esempi



Pharming e phishing: esempi

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

Pharming e phishing: esempi

Thunderbird ritiene che questo messaggio sia indesiderato.

Salve!

Come avrai già indovinato, il tuo account [redacted] è stato hackerato, perché è da lì che ho inviato questo messaggio. :(

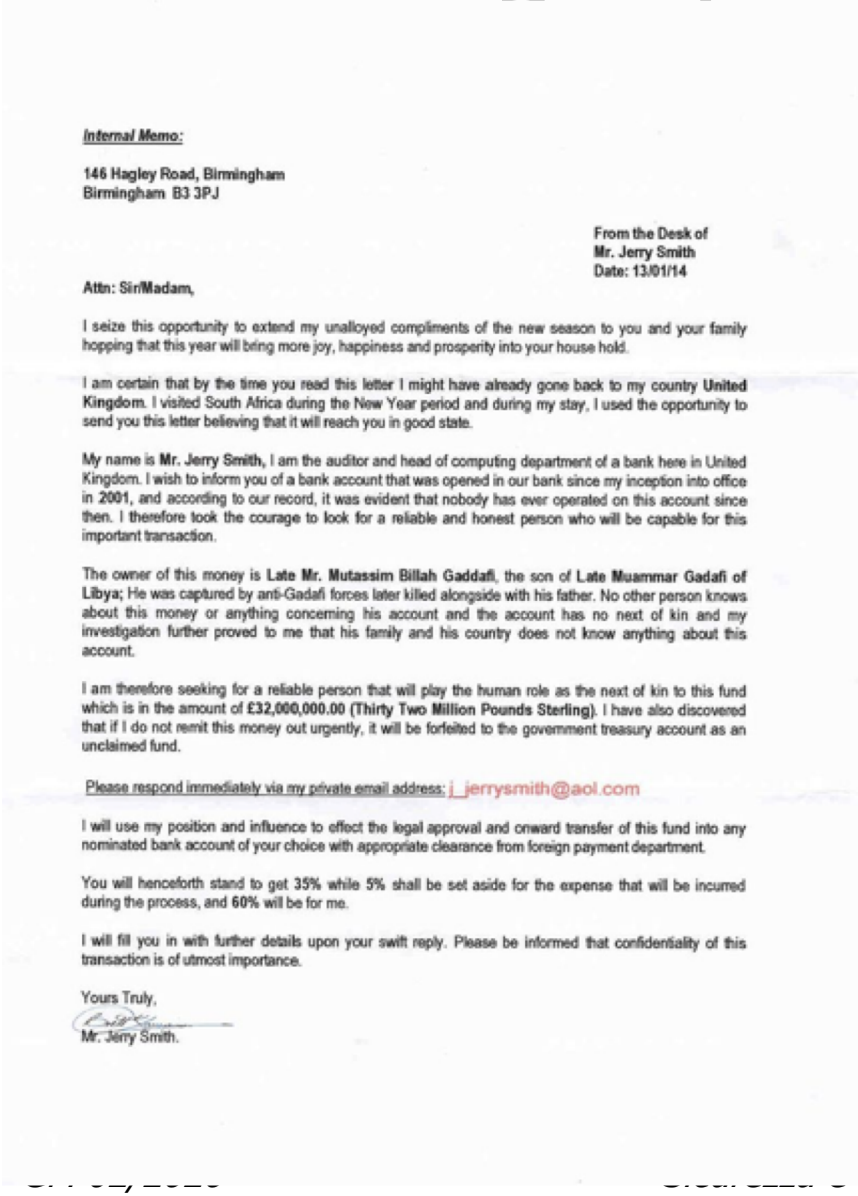
Io rappresento un gruppo internazionale famoso di hacker.
Nel periodo dal 22.07.2018 al 14.09.2018, su uno dei siti per adulti che hai visitato, hai preso un virus che avevamo creato noi.
In questo momento noi abbiamo accesso a tutta la tua corrispondenza, reti sociali, messenger.
Anzi, abbiamo i dump completi di questo tipo di informazioni.

Siamo al corrente di tutti i tuoi "piccoli e grossi segreti", sì sì... Sembra che tu abbia tutta una vita segreta.
Abbiamo visto e registrato come ti sei divertito visitando siti per adulti... Dio mio, che gusti, che passioni tu hai... :)

Ma la cosa ancora più interessante è che periodicamente ti abbiamo registrato con la web cam del tuo dispositivo, sincronizzando la registra
Non credo che tu voglia che tutti i tuoi segreti vedano i tuoi amici, la tua famiglia e soprattutto la tua persona più vicina.

Trasferischi 300$ sul nostro portafoglio di criptovaluta Bitcoin: 1LXxZyP7CKybaXA6jELu5YJ6UQzbdZz8RP
Garantisco che subito dopo provvederemo a eliminare tutti i tuoi segreti!
Dal momento in cui hai letto questo messaggio partirà un timer.

Pharming e phishing: esempi



Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hopping that this year will bring more joy, happiness and prosperity into your house hold.

I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith,** I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Billah Gaddafi**, the son of **Late Muammar Gadafi of Libya;** He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: j_jerrysmith@aol.com

I will use my position and influence to effect the legal approval and onward transfer of this fund into any nominated bank account of your choice with appropriate clearance from foreign payment department.

You will henceforth stand to get **35%** while **5%** shall be set aside for the expense that will be incurred during the process, and **60%** will be for me.

I will fill you in with further details upon your swift reply. Please be informed that confidentiality of this transaction is of utmost importance.

Yours Truly,
Mr. Jerry Smith.

Truffa alla nigeriana

Precauzioni - OTP

- One Time Password (OTP)
  password aggiuntiva, usa-e-getta, di durata limitata, generata al volo da un'App per smartphone o inviata all'utente tramite SMS
- Impedisce che un'eventuale intercettazione della connessione fra il computer ed il server possa rivelare tutti gli elementi di identificazione necessari
- Se anche dovesse essere intercettata, non è riutilizzabile una seconda volta

TWO FACTOR AUTHENTICATION

Vulnerabilità

Si dicono **Vulnerabilità** quegli errori di progettazione e di realizzazione presenti all'interno dei programmi che utilizziamo

Attenzione: TUTTI i programmi! Compresi il sistema operativo, i driver, le estensioni del vostro browser, le utility!

Le vulnerabilità vengono eliminate tramite gli **aggiornamenti software**

Solitamente non hanno conseguenze sulla sicurezza

Alcune, però, possono essere sfruttate per sferrare attacchi (p.es. accessi non autorizzati)

Alla fine delle slide ho approfondito un po'.

Hoax e SPAM

Per **Hoax** si intendono notizie false (bufale)

Per **Catene di Sant'Antonio** si intendono messaggi che si diffondono creando false emergenze e chiedendo a chi li riceve di essere inviati a più persone possibile.

Per **SPAM** si intende l'invio in grande quantità di messaggi di posta elettronica, tipicamente a scopo pubblicitario o di Phishing

In generale né Hoax né SPAM rappresentano problemi per la sicurezza, ma sovraccaricano la rete e fanno perdere tempo

Possono però essere utilizzati per veicolare messaggi fuorvianti (false notizie, credenze, ecc) con gli scopi più vari (p.es. orientamento elettorato)

Cookie

I **Cookie** (dall'inglese, "biscotto") sono piccoli file di testo creati sul computer dell'utente quando visita una pagina web

Sono nati per memorizzare preferenze (p.es. la lingua preferita, il contenuto del carrello, ecc) e quindi facilitare la navigazione

Un utilizzo improprio dei cookies può compromettere la riservatezza della propria sfera privata, rendendo possibile il tracciamento delle attività dell'utente

Chat e Instant Messaging

Per la loro apparente anonimità, i servizi chat (o di instant messaging) vengono spesso sfruttati per operazioni illegali (ad esempio adescamento)

Possono inoltre essere utilizzati come vettori di infezione (virus, worm o trojan) quando i partecipanti alla chat sono invitati a cliccare su link o a digitare comandi sconosciuti

Chat e Instant Messaging

Esistono MANUALI sul Dark Web che insegnano a come comportarsi per adescare adolescenti. Insegnano come rispondere, cosa scrivere, come scriverlo, quali orari avere...

Quindi STATE ATTENTI, non fidatevi mai se non avete riscontro diretto e sicuro della persona a cui state parlando!

Adescamento online

GUARDATE BENE QUESTO VIDEO

https://www.youtube.com/watch?v=X002HMDHVJY

Wireless LAN (WiFi)

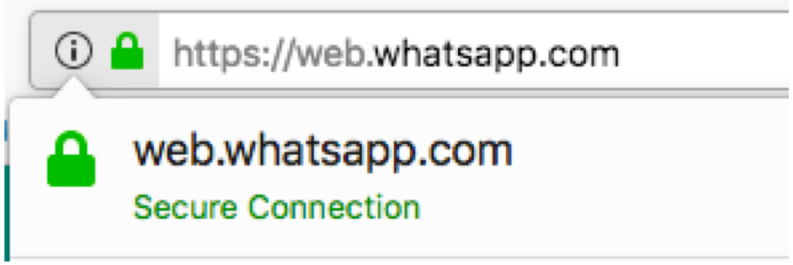
Una configurazione imprudente del WLAN Access Point può determinare l'accesso illimitato a persone non autorizzate rendendo possibile l'accesso al computer e ai dati e l'uso abusivo del collegamento a internet.

La cifratura insufficiente dei collegamenti WLAN consente la lettura dei dati scambiati tra gli apparati ed i router attraverso strumenti relativamente semplici.

Wireless LAN (WiFi)

Ma anche i collegamenti WLAN cifrati possono essere intercettati se qualcuno riesce a connettersi alla rete.

Per questo motivo, quando si è connessi a reti WiFi (private ma soprattutto pubbliche) è buona norma navigare solo su siti sicuri, contraddistinti dal prefisso "**https:**" ed accertarsi che il "**lucchetto**" sia chiuso.



Altre misure di sicurezza (Wikipedia)

Protezioni e precauzioni

- Firewall
- Aggiornamenti software (Software Update)
- Antivirus (sempre aggiornato!)
- Backup (Sistema e Dati)
- Scelta delle password
  - min 8 caratteri, minuscole, maiuscole, cifre, segni
  - facili da ricordare, difficili da indovinare
  - un servizio, una password
  - modificate di frequente

Precauzioni - Backup

- Si dice backup una copia di sicurezza dei dati e/o dell'intero sistema
- Protegge dalla perdita dei dati per qualsiasi causa (p.es. guasto HW, distrazione, ransomware)
- Va eseguito periodicamente (ogni giorno/ settimana/ mese a seconda delle esigenze)
- Su un dispositivo esterno (Hard Disk, nastro, supporto ottico, cloud)
- Il backup deve essere tenuto in un luogo sicuro e lontano dal computer
- Deve essere verificato eseguendo di tanto in tanto la procedura di ripristino

Precauzioni - Browser

- Eliminare i dati privati dal browser
  - cronologia
  - credenziali (utente e password) per fare login su siti web
  - dati per il completamento automatico dei moduli
- Disattivare il completamento automatico da parte del browser (soprattutto se il computer è usato da più persone):
  - credenziali di login
  - riempimento di moduli

Precauzioni - Email

- Mittente ignoto o sospetto: non aprire allegati e non cliccare sui link
- Non visualizzare automaticamente contenuto remoto
- Aprire solo messaggi di fonte certa (evt. verificare prima di aprire) e filtrati da antivirus
- Fare attenzione alle doppie estensioni (sexyphoto.jpg.exe)

Precauzioni - Email

- Mantenere aggiornato il client di posta
- Limitare la diffusione dei propri indirizzi
- Se possibile usare indirizzi "a perdere" per non mettere a rischio l'indirizzo primario
- Non rispondere allo SPAM
- Risposta automatica (p.es. in caso di assenza) solo per mittenti conosciuti
- Non partecipare alle catene di Sant'Antonio (semmai rispondere al mittente, se conosciuto)

Precauzioni - Navigazione

- Non scaricare programmi sconosciuti
- Scaricare ed aggiornare i programmi solo dai siti dei produttori
- Non comunicare a nessuno le proprie credenziali di accesso ai servizi
- Utilizzare carte di credito solo su siti sicuri (https) e di nota reputazione
- Uscire sempre da un'applicazione (logout, exit, signout) prima di liberare una postazione di lavoro condivisa
- Configurare il browser in modo da limitare i rischi legati a componenti dinamiche (Java, Flash, ecc) e la raccolta di dati personali (cookie)

Precauzioni - Social Network

- Non divulgare informazioni riservate sui social network
- Applicare impostazioni adeguate per salvaguardare la privacy del proprio account
- Idealmente, rendere accessibile il proprio profilo solo a persone che si conoscono anche nella vita reale
- Ricordare che, in caso di molestie, si può sempre:
  - Segnalare l'abuso
  - Bloccare l'utente
  - Uscire dal social network
  - Denunciare l'accaduto alle autorità

Privacy

Per privacy si intende "il diritto di controllare l'uso e la circolazione dei propri **dati personali** che costituiscono il bene primario dell'attuale società dell'informazione" *(Garante Privacy)*

Dati Personali

I **dati personali** identificano le informazioni relative alla persona fisica, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altro dato, ivi compreso un numero di riconoscimento personale.

Ci sono vari tipi di dati personali:

- Dati Identificativi
- Dati Sensibili (o Particolari)
- Dati Giudiziari

Dati Identificativi

Sono i dati personali che permettono l'identificazione diretta dell'interessato.

Principali **dati identificativi**:

- Nome
- Cognome
- Data di nascita
- Luogo di nascita
- Codice Fiscale

Dati Sensibili (particolari)

Sono dati personali la cui raccolta e trattamento sono soggetti sia al consenso dell'interessato sia all'autorizzazione preventiva del Garante per la protezione dei dati personali

Principali **dati sensibili** sono quelli inerenti:

- origine razziale/etnica
- convinzioni religiose
- opinioni politiche
- vita sessuale
- salute (dati sanitari)
- dati biometrici (foto viso, impronte dita, iride)
- dati genetici (DNA)

Dati Giudiziari

Sono dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti.

Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato

Principali diritti

Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Conosci i principali diritti previsti dal Regolamento (UE) 2016/679?

Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).

Accesso ai propri dati personali

Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.

Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali

Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati.

Opposizione al trattamento

Puoi opporti al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.

Come si esercitano questi diritti?

Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile). Il titolare del trattamento è tenuto entro 1 mese a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.

Scopri di più su: www.garanteprivacy.it/home/diritti

La crittografia

https://www.youtube.com/watch?v=EerThGU6smg

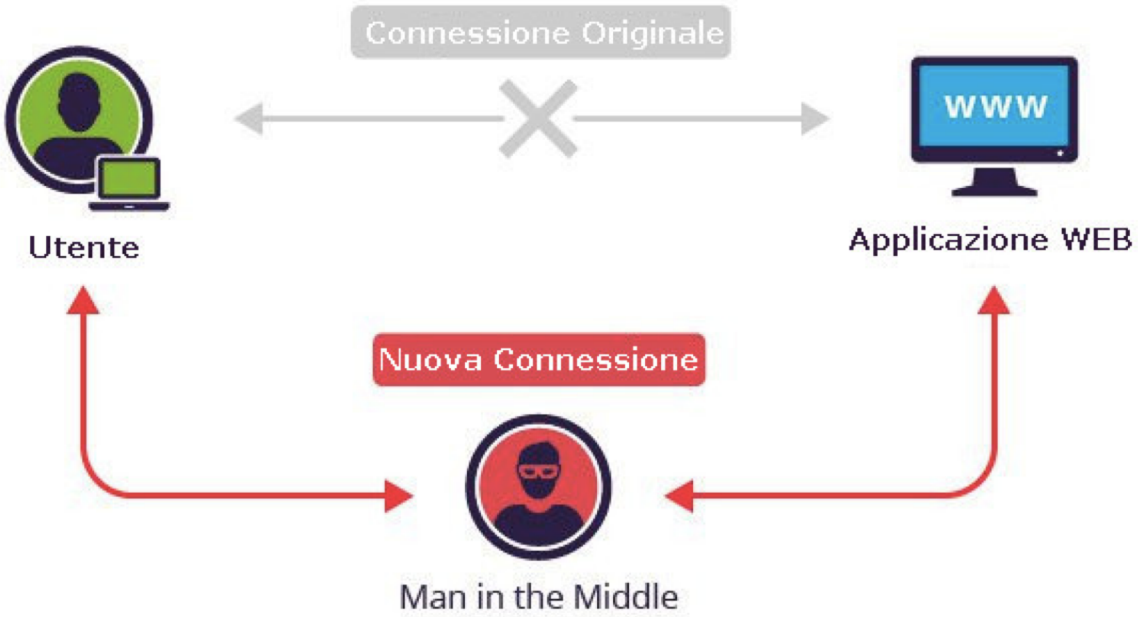
Enigma: https://www.youtube.com/watch?v=EVvrSjah9t0

Crittografia e numeri primi: https://www.youtube.com/watch?v=nJyeeAqneeQ

Crittografare dati significa codificarli in maniera tale che siano leggibili solo da chi è in possesso della chiave.

Serve a proteggersi non solo da eventuali malware presenti sul computer che potrebbero accedere a tali dati, ma anche a difendere i dati dal cosiddetto «Man in the middle»

Man-In-The-Middle



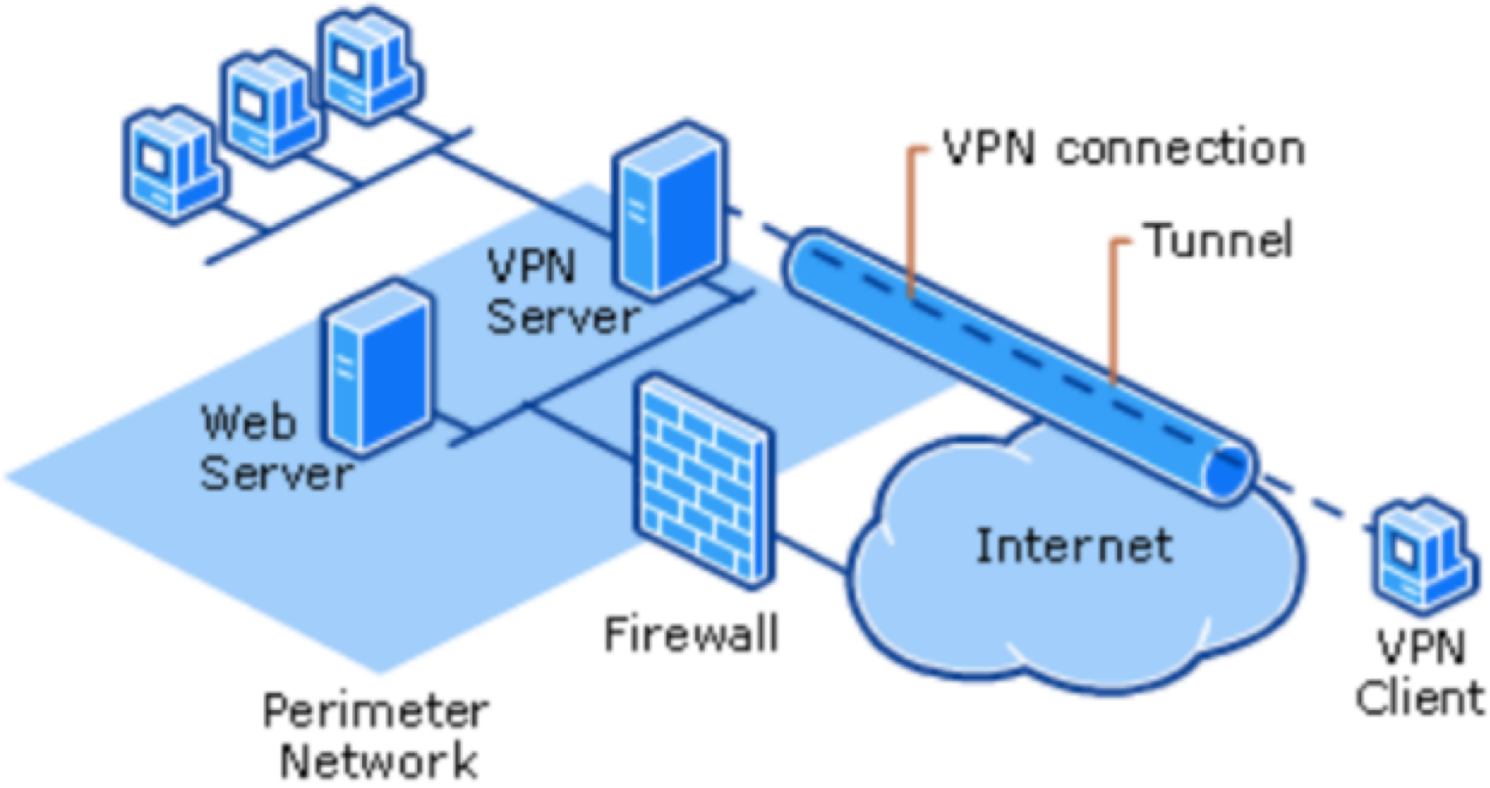
https://apolis.it/2019/09/man-in-the-middle-come-funziona/

Man in the middle è un attacco che avviene esternamente al nostro computer. Per difenderci dobbiamo usare la crittografia.

Man-In-The-Middle

- Utilizziamo quando possibile https invece di http
- se necessario adottiamo una VPN (Virtual Private Network)

Approfondimento: VPN



Come gentilmente richiesto...

- Lo SPAM telefonico. Come difendersi?
  - Si tratta di una odiosa pratica (illegale).
  - Potete iscrivervi al registro delle opposizioni (http://www.registrodelleopposizioni.it/)
  - Potete installare una app che vi protegga come TrueCaller (https://play.google.com/store/apps/details?id=com.truecaller&hl=it)

Approfondimento: hacker bianchi e neri

Al mondo esistono i cosiddetti hacker **bianchi** e gli hacker **neri** (che per fortuna sono di meno).

Entrambi lavorano incessantemente per cercare **vulnerabilità** nei software, ovvero errori che possano essere sfruttati per compiere azioni malevole.

Quando un hacker trova una vulnerabilità cerca anche il modo di farne un cosiddetto **exploit**, ovvero di sfruttarla per compiere azioni malevole, dopodiché agisce di conseguenza:

Se è un hacker nero, cerca di tenere il segreto e sfruttarlo per scopi loschi.

Se è un hacker bianco, lo comunica alle aziende di antivirus perché possano proteggere i computer da questa vulnerabilità, ed agli sviluppatori perché possano correggere l'errore attraverso un update. Rendendo però pubblico il rischio, che a questo punto potrà essere sfruttato anche da hacker neri che non avevano scoperto la vulnerabilità in precedenza.

Per questo motivo è FONDAMENTALE che le applicazioni e l'antivirus siano aggiornati, è in corso una vera e propria gara di velocità e aggiornare il software è l'unica possibilità che abbiamo per difenderci.

Approfondimento: vulnerabilità

https://encyclopedia.kaspersky.it/knowledge/vulnerabilities-examples/

Un esempio tipico di vulnerabilità è un cosiddetto **buffer overrun**. Caso: un software richiede l'inserimento di un testo (ad esempio un nome di utente, il nome del progetto, una email...). Il programmatore potrebbe non aver implementato alcuni controlli: ad esempio non preoccuparsi di verificare che i dati inseriti non possano eccedere una certa lunghezza.

Se inserissi, come nome utente, un testo di un milione di caratteri, contenenti anche dati non testuali? Il programma potrebbe andare a scrivere questi caratteri in aree di memoria che non erano dedicate al nome utente e quindi creare danni o addirittura attivare un malware.

Un altro mancato controllo tipico è nei confronti di caratteri speciali, come è successo a WhatsApp (che bloccava tutti gli iPhone e iPad) nel 2018, con uno speciale carattere hindi:

https://www.youtube.com/watch?v=K73fw99Xb9s

Approfondimento: Malware nei diversi s/o

Microsoft Windows è il sistema operativo più usato al mondo.

Per questo motivo la gran parte dei malware è per Windows o per sue applicazioni: semplicemente perché è più economico, per un hacker, infettare computer Windows, essendocene molti di più.

A questo si aggiunge che, purtroppo, Microsoft ha spesso dimostrato scarsa cura alla sicurezza nei propri software e scarsa velocità negli update, anche se ultimamente il suo comportamento è sensibilmente cambiato.

In realtà, comunque, malware esistono per tutti i sistemi operativi e per moltissime applicazioni. Anche Android, iOS, MacOS, Linux e Unix hanno malware e vulnerabilità, solo molto meno.

Almeno fino al 2019, anno in cui Mac ha superato Windows in quanto a malware (compresi adware) rilevati!

C'è da tenere presente che Android e iOS, comunque, sono sistemi operativi molto più recenti, che adottano tecniche di protezione moderne che erano impensabili anni fa. Ad esempio, una app su Android ha accesso **estremamente** limitato al vostro sistema e ciò rende «quasi» impossibile che una app, anche se infetta, possa riuscire a creare danni.

Approfondimento: Statistiche malware

Windows threat landscape 2019

Global detections 2018-2019

	2018	2019	% Change
Overall	50,170,502	50,510,960	1%
Business	8,498,934	9,599,305	13%
Consumer	41,671,568	40,911,655	-2%

Figure 1. Total number of consumer and business detections in 2019 vs. 2018

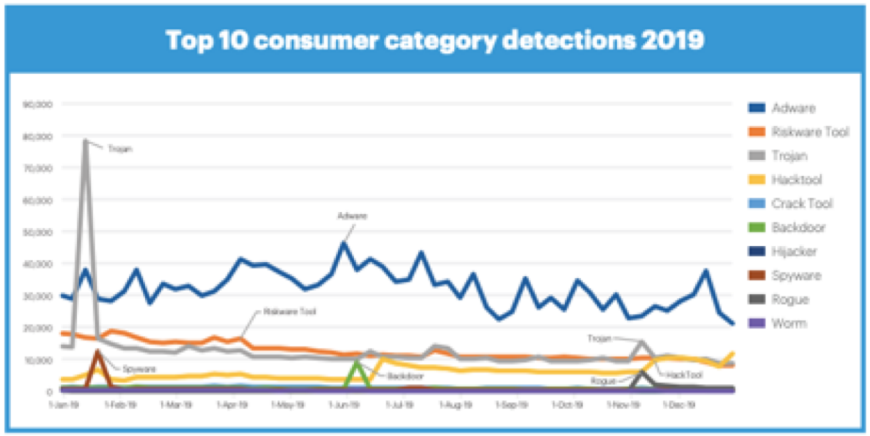


Figure 2. Top 10 consumer threat categories in 2019

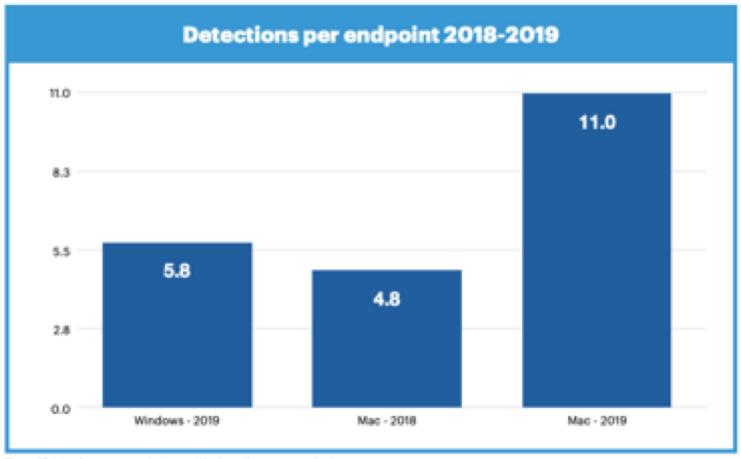


Figure 18. Mac threats per endpoint vs. Windows threats per endpoint

<-- Il Mac supera Windows

Fonte: Malwarebytes

Approfondimento: iOS e Android

Secondo Malwarebytes, iOS e Android sono anche essi affetti da malware, vediamo cosa dice nel report di fine 2019.

iOS: a quanto sostiene Malwarebytes, vulnerabilità e malware in grado di sfruttarle esistono su iOS, ma è impossibile fare una scansione per trovarle. Il *jailbreak* (ovvero un sistema per bypassare il sistema operativo sfruttando un bug nello stesso) del 2019 è derivato da un bug addiritura nella ROM, presente su una marea di dispositivi da iPhone 4S fino a iPhone X, watchOS, tvOS ecc., e che, essendo nella ROM (Read Only Memory) non può essere risolto se non comprando un nuovo telefono.

Android: Malwarebytes ha trovato trojan *pre-installati* (inconsapevolmente?) in alcuni telefoni Android e spesso impossibili da rimuovere, intenti a rubare dati personali per un totale di più di 300.000 scoperte in un anno! C'è inoltre allarme per quasi altrettante app contenenti un Hidden Ads, un malware in grado di far comparire pop-up di pubblicità.

Fonte: Malwarebytes

Approfondimento: Ancora malware

I malware si possono nascondere in siti, immagini, mail, perfino nell'hardware, con tecniche sempre più evolute. Invito tutti a leggere il report 2019 qui allegato:

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

Fonte: Malwarebytes

Approfondimento: I migliori antimalware

I migliori antimalware (o antivirus) devono:

- Essere efficaci nel riconoscimento dei pericoli
- Avere pochi falsi positivi (errori di valutazione nei confronti di file legittimi, riconosciuti come malware)
- Proteggere anche sul web e sulla mail
- Sottoporre il computer a carico non troppo elevato

Potete accedere al sito https://av-test.org per avere un'idea di quali siano gli antivirus più efficaci nell'ultimo periodo. In genere (in ordine):

Windows: Kaspersky, Norton, Avira, VIPRE, McAfee, BitDefender

Mac: BitDefender, Norton, Kaspersky, TrendMicro

Android: BitDefender, TrendMicro, Gdata, Kaspersky, McAfee, Norton

Fonte: av-test.org

Approfondimento: SQL Injection

Un attacco che sfrutta un errore del codice, per cui quando viene richiesto di inserire un testo (ad esempio un nome), viene inserito un testo «trappola» che verrà interpretato dal programma o dal sito (se scritto senza attenzione) come un comando da eseguire, in particolar modo per distruggere un database.

Approfondimento: SPAM

L'origine della parola SPAM è incredibile.

Deriva da uno sketch comico del gruppo inglese *Monty Python*, che raffigura un ristorante in cui qualsiasi voce del menu contiene carne in scatola Spam (realmente esistente).

https://www.youtube.com/watch?v=_bW4vEo1F4E

Approfondimento: Mitnick

https://www.youtube.com/watch?v=HNyRcYZws98

Mitnick è uno dei più noti hacker di tutti i tempi, ed ha usato spesso, oltre alle sue capacità informatiche, anche tecniche di social engineering.

Approfondimento: Snowden

https://www.youtube.com/watch?v=Weq0myVo2M8

Snowden (di cui vi consiglio il film biografico) è un hacker che, dopo aver lavorato per la CIA, ha deciso di renderne pubblici alcuni comportamenti scorretti, tra cui l'aver creato un *worm* in grado di spiare gli utenti attraverso la telecamera.

Approfondimento: Assange

https://www.youtube.com/watch?v=2Wf0jlxjNiY

Assange ha creato Wikileaks, un sito dove svariati documenti segreti (spesso folti di informazioni scottanti) sono stati pubblicati in seguito ad attacchi hacker o semplici furti. E' giusto o non è giusto pubblicare simili documenti? Domanda aperta...