Divulgazione Informatica

Gli attacchi informatici e come proteggerci

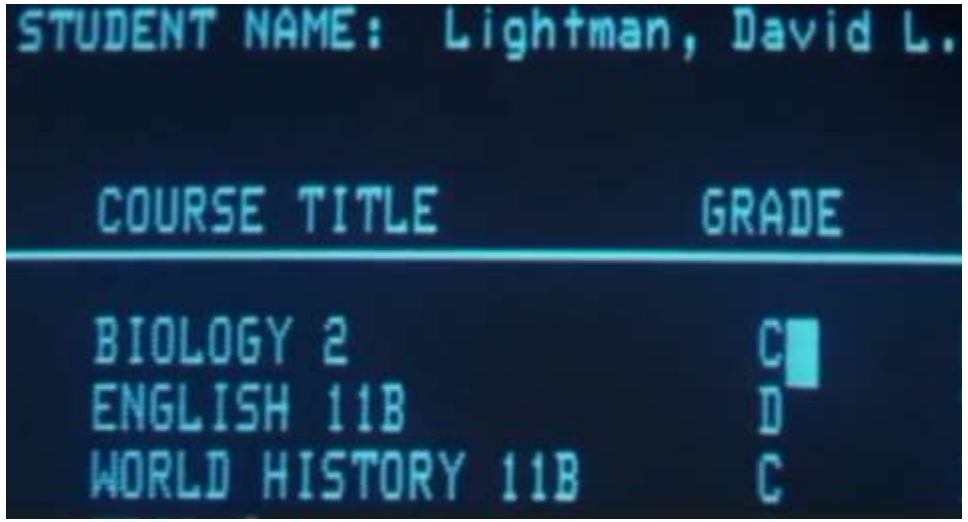
Gennaio 2025

Di cosa parleremo

- **Hacker e tipi di attacchi informatici**
- **I punti vulnerabili del dispositivo (PC, Tablet, Smartphone)**
- **Come difendersi:**
  - **gli strumenti**
  - **le regole di comportamento**
- **Le truffe informatiche più comuni**

Gli Hacker

Come non ricordarlo…..



WarGames – Trailer in italiano

Il fenomeno degli hacker: gli inizi

Hacker: derivato dal verbo inglese "to hack" che significa "tagliare", "sfrondare", "ridurre", "aprirsi un varco“.

In origine (anni ‘80-’90) ***Hacker*** era chi, utilizzando le proprie conoscenze informatiche, modificava il codice dei programmi per rendere più efficiente e veloce il software esistente.

Il fenomeno degli hacker: gli inizi

L'hacking non nasce quindi con intenti criminali; a volte si sviluppa per compiacere la propria bravura ed il proprio divertimento.

L'Hacker non aveva un fine malevolo, ma ha dato origine ad una consapevolezza: "*con le opportune conoscenze il software può essere violato*".

L’evoluzione dell’Hacking

Se prima l'hacking era un dispetto compiuto da ragazzini, oggi è un'attività che rende miliardi di dollari.

Oggi si definiscono spesso l'hacking e gli hacker come attività e soggetti che operano nell'illegalità, criminali informatici che agiscono per ottenere:

- un **guadagno finanziario**, commettendo il furto di numeri di carte di credito o truffando i sistemi bancari
- **fama e reputazione** nella sottocultura degli hacker, allo scopo di lasciare "firme" sui siti vandalizzati solo per dare prova di essere riusciti nell'impresa
- **spionaggio aziendale**, che riguarda il furto di informazioni relative a prodotti e servizi aziendali da parte di concorrenti per ottenere un vantaggio sul mercato
- **dati di intelligence nazionale** con l'obiettivo di destabilizzare l'infrastruttura degli avversari o per seminare discordia e confusione nel Paese colpito

L’evoluzione dell’Hacking

Esiste ancora un'altra categoria di criminali informatici: gli hacker spinti da una motivazione sociale o politica, per esempio:

- Anonymous
- WikiLeaks
- LulzSec

L'Hacker come professione (ben retribuita!)

L'***hacker***, nel suo aspetto positivo (Hethical Hacker o Hacker bianco), è una vera e propria professione, anche pagata molto bene!

Dal punto di vista professionale viene utilizzato all'interno di aziende o istituzioni per identificare le esposizioni di sicurezza in un sistema informatico e correggerle prima che lo possano fare i male-intenzionati.

Essi svolgono una serie di attività di hacking lecite e utili sottoponendo i sistemi informatici a test al fine di valutarne e comprovarne sicurezza e affidabilità agendo nella ricerca di potenziali falle.

Gli attacchi informatici

Le tipologie di attacchi informatici

I **Malware,** termine generico contrazione di **Mal**icious Soft**ware,** sono quei programmi che hanno lo scopo di provocare danni ai nostri dispositivi: computer, smartphone, tablet.
Fra i principali malware vi sono:

- i **Virus**: solitamente piccoli (per passare inosservati) che si nascondono in altri programmi o documenti, in grado di autoreplicarsi e diffondersi (tramite internet o chiavette USB o dischi esterni)
- le **Backdoor**: che consentono di prendere il controllo del nostro computer da parte di un hacker tramite internet
- i **Trojan** (cavalli di Troia): programmi che installiamo volontariamente sul computer ed attivano poi Virus o Backdoor

Le tipologie di attacchi informatici

Fra i **Virus** più pericolosi etichettiamo due tipi:

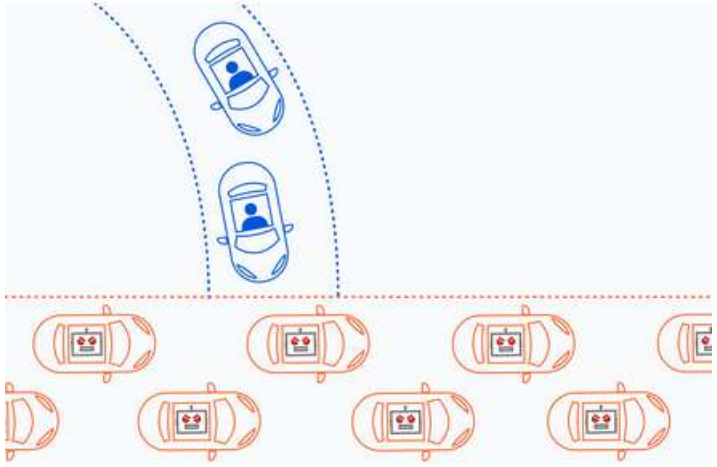
- i **Virus Ransomware**: che cifrano i dati della vittima e chiedono un riscatto, quindi un pagamento, per fornire la chiave necessaria a decifrarli

- i **Virus Spyware**: si tratta di virus progettati con lo scopo di collezionare, usare e diffondere i dati personali della vittima.

Le tipologie di attacchi informatici

Una altro tipo di attacco finalizzato a '*mettere in ginocchio*' una istituzione o unaazienda attaccata è il **Distributed Denial of Service** (**DDoS**), mal-tradotto come 'intralcio al servizio'.

In questi attacchi gli hacker agiscono memorizzando su migliaia di dispositivi un virus dormiente che servirà a scatenare l'attacco in un giorno prestabilito (meccanismo di innesco a tempo detto *Time Bomb*).



Quando parte l'attacco i computer infetti eseguono una enorme quantità di richieste sul sito web dell'azienda o istituzione sotto attacco con conseguente collasso e chiusura del servizio.

Il danno economico, ma soprattutto di immagine, può essere ingente.

Le tipologie di attacchi informatici

L’attacco che più ci impatta come utenti di dispositivi informatici e che non si avvale di strumenti (antivirus) in grado di combatterlo è il

PHISHING

La tecnica del phishing consiste nell’inviare mail, SMS, messaggi Whatsapp contenenti comunicazioni fraudolente che sembrano provenire da una fonte reale.
L’obiettivo di questo attacco è carpire i dati sensibili della vittima (ad esempio: carte di credito, carta d’identità o passaporto, credenziali di accesso) o di installare sul dispositivo un virus con cui prenderne il controllo.

Le tipologie di attacchi informatici

Poiché le password sono il meccanismo più comunemente usato per autenticare gli utenti a un sistema informatico o ad un sito, **ottenere le password** è un approccio di attacco comune ed efficace.

Indovinare la password con la **forza bruta** significa usare un programma che genera e prova diverse password in modo casuale sperando che una funzioni. L'hacker applica una certa logica, provando password legate al nome della persona, alla data di nascita, al lavoro, agli hobby, alla squadra del cuore ed elementi simili.

Per proteggersi dagli attacchi alle password è necessario implementare una politica di blocco dell'utente che interviene dopo alcuni tentativi di password non valide.

Alcuni attacchi informatici passati alla storia

Wannacry

E’ un virus responsabile di un‘epidemia su larga scala avvenuta nel maggio 2017 su computer con Microsoft Windows.

Una volta installato nel computer, il virus si va a "posizionare" all’interno del sistema operativo Windows e da qui prima crittografa alcune tipologie di file e poi passa a infettare tutti gli altri computer a cui il computer infettato è connesso. Si diffonde velocemente e crittografa i file della rete aziendale in poco tempo, rendendo inutilizzabili i computer.
L’attacco aveva l’obiettivo di chiedere un riscatto per ottenere la chiave di crittografica per recuperare i file.

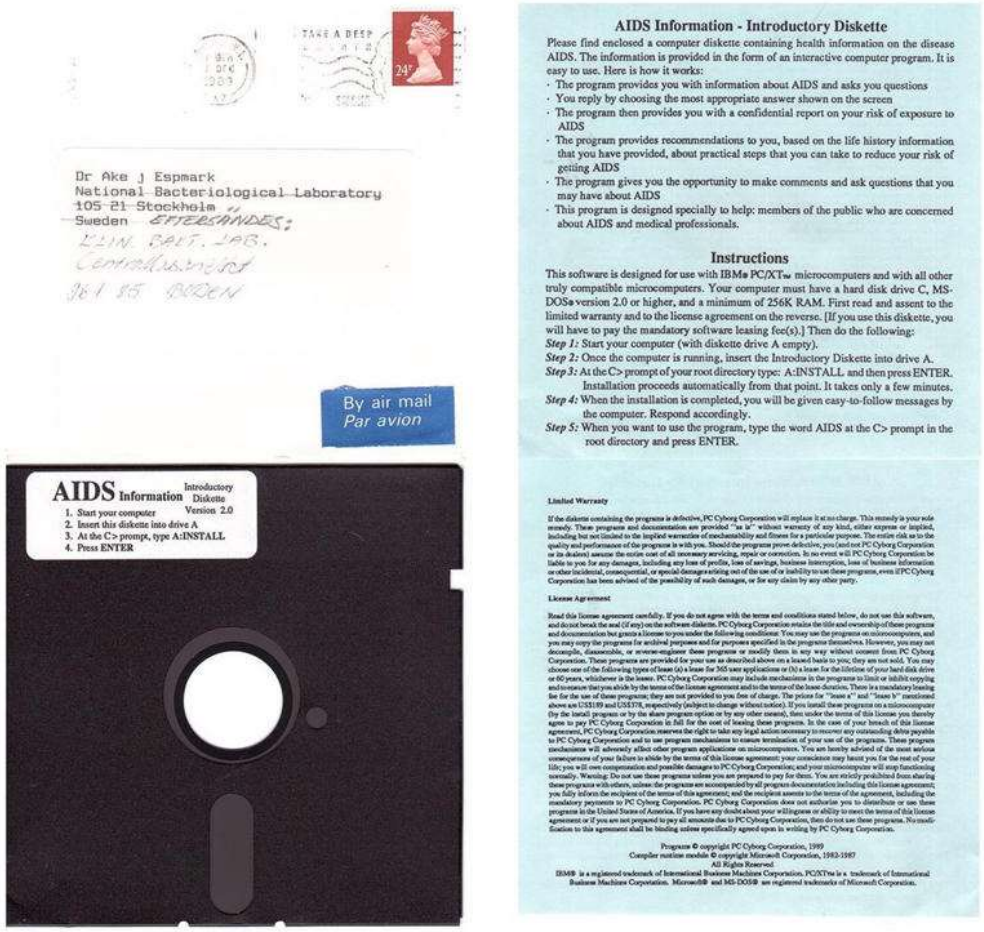
A fine Maggio 2017 erano stati colpiti circa 300.000 computer in 150 paesi, rendendolo uno dei maggiori contagi informatici mai avvenuti.

Alcuni attacchi informatici passati alla storia

Wannacry

Il primo ramsomware della storia

Verso la fine del **1989**, un oggetto apparentemente innocuo, un **floppy disk da 5,25 pollici**, ha dato avvio a una delle più grandi minacce per la sicurezza informatica mondiale.
Quel dischetto era etichettato come "*AIDS Information – Introductory Diskette 2.0*" prometteva di veicolare informazioni sulla nota malattia. In realtà, era il primo esempio di un attacco informatico volto a bloccare i dati delle vittime e a chiedere un **riscatto** per il loro "rilascio".

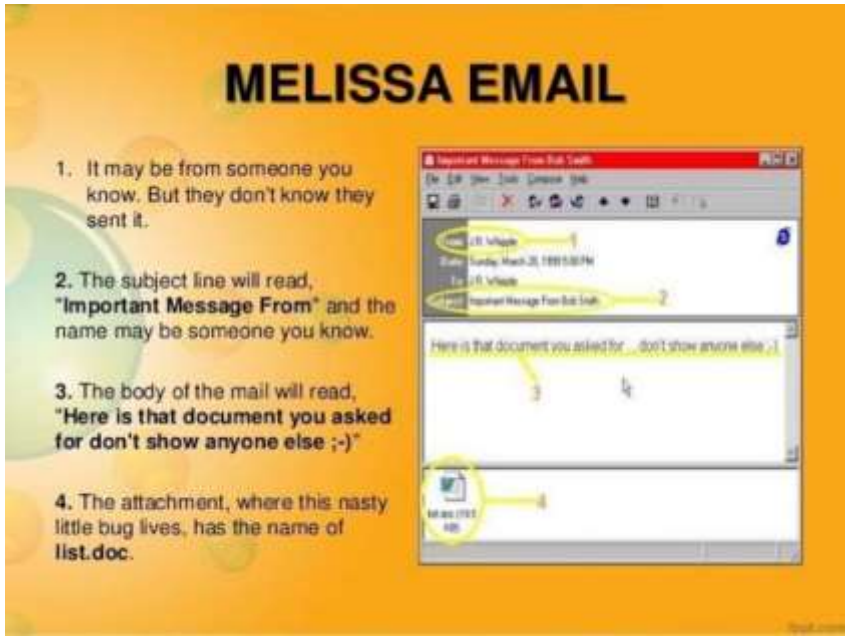


Alcuni attacchi informatici passati alla storia

Melissa

Un **virus che ha causato danni per oltre 1 miliardo di dollari;** si è diffuso nel 1999 **colpendo i sistemi operativi Windows**, attraverso i file Microsoft Word e il servizio di posta elettronica Outlook.

Il virus Melissa infettava i documenti con estensione *.doc* e attraverso il client di posta *Outlook* si auto-inviava ai primi 50 contatti presenti in rubrica, espandendosi così a macchia d'olio.



Alcuni attacchi informatici passati alla storia

Stuxnet: le centrifughe d'uranio iraniane

Un altro **famoso attacco informatico**, e anche in realtà uno dei più pericolosi, è in realtà una vera e propria offensiva operata dal Governo americano e da quello israeliano **ai danni della centrale nucleare iraniana di Natanz**, attraverso un virus in grado di sabotare il software di gestione delle centrifughe e bloccarne la produzione.

Da Superquark (2011)

I punti vulnerabili dei dispositivi

Gli Attacchi Informatici

I punti vulnerabili del nostro PC o dello Smartphone

1. Allegati e-mail infetti

La maggior parte dei malware comuni arriva ad infettare il nostro PC o Smartphone attraverso la posta elettronica.
Solitamente l'attaccante invia un falso messaggio chiedendoci di aprire un allegato.

Proprio qui si nasconde il pericolo, infatti, **una volta aperto** il file, il virus finirà per installarsi sul dispositivo.

Gli Attacchi Informatici

I punti vulnerabili del nostro PC

2. Pendrive o altre unità rimuovibili infette

Le **chiavette USB** al contrario di quanto si pensi sono grandi **vettori di attacchi informatici mirati**, motivo per il quale le grandi aziende ne vietano l'utilizzo.

Le **pendrive infette** possono addirittura trasmettere un'infezione da virus anche solo dopo essere state inserite nel PC tramite un meccanismo chiamato ***Autoplay*** (se è presente un programma viene eseguito!).

Purtroppo molti utenti hanno la cattiva abitudine di "curiosare" sulle chiavette USB che trovano sparse in ufficio o magari che hanno trovato per strada.

Gli Attacchi Informatici

I punti vulnerabili del nostro PC o dello Smartphone

3. Siti web infetti

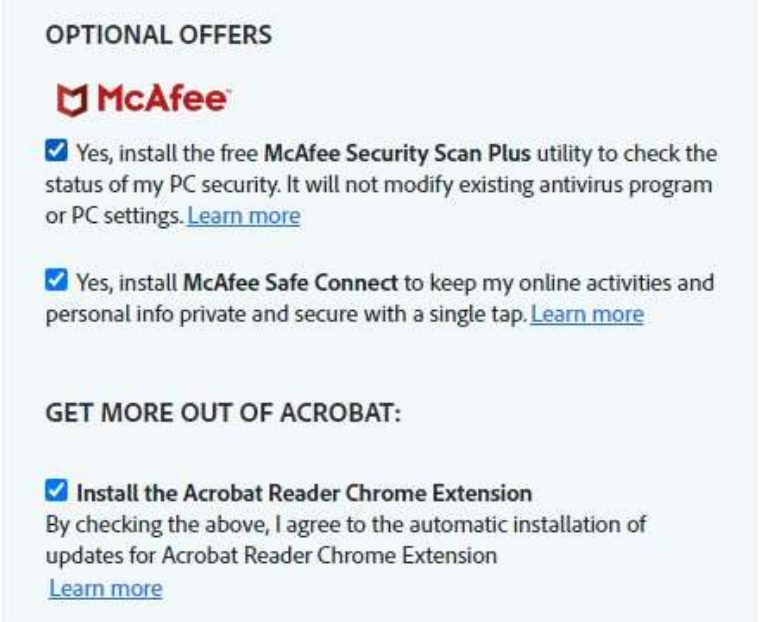
Tramite le pagine web violate da un hacker è possibile trasmettere malware alle proprie vittime. Questo accade perché i siti web spesso contengono vulnerabilità (dovute al mancato aggiornamento, alla mancanza di meccanismi di sicurezza, agli errori di configurazione, ecc) che se sfruttate da un attaccante possono compromettere la funzionalità delle pagine stesse.

Gli Attacchi Informatici

I punti vulnerabili del nostro PC o dello Smartphone

4. **Applicazioni o componenti software aggiuntivi**

Una **parte di virus informatici** infettano i dispositivi quando l'utente installa un software scaricato da Internet.
In alcuni casi, il software scaricato, soprattutto se non proveniente da 'App Store' certificate, include pezzi di programma che potrebbero nascondere un virus.



I sintomi che indicano la presenza di un virus informatico

Molti virus informatici lavorano in sordina, senza dare nell'occhio e soprattutto senza sintomi per il dispositivo infetto.

Tuttavia, la stragrande maggioranza dei **virus informatici** quando entra in azione genera una serie di comportamenti anomali sul dispositivo colpito.

Vediamo dunque quali sono i comportamenti dei nostri dispositivi che dovrebbero metterci in allarme e che quasi certamente indicano una contaminazione **da virus.**

I sintomi che indicano la presenza di un virus informatico

1. Calo improvviso delle prestazioni

Se vi rendete conto che qualcosa è improvvisamente cambiato nel comportamento del vostro dispositivo molto probabilmente qualcosa non va per davvero.

Chi meglio conosce un computer o uno smartphone del suo stesso utilizzatore?

Un dispositivo che è stato infettato con un virus impiegherà **molto tempo per aprire le applicazioni** o per eseguire qualsiasi tipo di comando. Questo accade perché i virus **sfruttano parte della potenza elaborativa del dispositivo** per funzionare.

I sintomi che indicano la presenza di un virus informatico

2. Comparsa di nuovi software

Se notate la comparsa di nuovi programmi o applicazioni che non avete mai scaricato molto probabilmente si tratta di malware o di applicazioni indesiderate.

Molto spesso questi software s'installano in accompagnamento ad altri programmi che avete scaricato gratuitamente da Internet.

Non sempre si tratta di virus informatici ma può anche trattarsi di software che sottraggono risorse al vostro computer per supportare l'attività illegale degli hacker (per esempio sfruttare il dispositivo per un'attacco DDOS).

I sintomi che indicano la presenza di un virus informatico

3. Azioni incontrollate del dispositivo

Alcuni virus informatici possono eseguire in autonomia alcune azioni sui PC (meno frequentemente sugli smartphone) tra cui:

- il computer si arresta e si riavvia da solo;
- non è possibile avviare il sistema operativo;
- il computer va in crash frequentemente (schermata blu);
- i comandi associati ai tasti del mouse sono invertiti;
- il puntatore mouse si muove da solo;
- i programmi si aprono, chiudono o riavviano da soli senza motivo;
- ecc. …

I sintomi che indicano la presenza di un virus informatico

4. Comparsa di avvisi pubblicitari invadenti o notifiche sul desktop

Siamo talmente abituati ad essere bombardati da avvisi, pubblicità e notifiche da non renderci conto quando questa situazione diventa potenzialmente pericolosa. Ebbene, molti virus informatici si nascondono dietro i messaggi pubblicitari (presenti in applicazioni adware, ovvero supportate da pubblicità) e le notifiche, e hanno come obiettivo quello di reindirizzare la nostra navigazione internet verso siti web infetti.

I sintomi che indicano la presenza di un virus informatico

5. Consumo anomalo della batteria dello smartphone

Se verifichiamo che la batteria del dispositivo si scarica più frequentemente del solito probabilmente un'applicazione la sta utilizzando in modo anomalo e potrebbe essere un virus.
Può essere utile effettuare una rapida verifica relativamente alle **app che consumano più batteria**. Infatti, alcune soluzioni malevole lavorano "sottobanco" (background) andando dunque a impattare in modo importante sull'autonomia.
Sia da **Android** che da **iPhone** è possibile visualizzare le applicazioni più "fameliche"; basta seguire il percorso **Impostazioni -> Batteria** (eventualmente premendo anche sull'opzione **Utilizzo batteria**) ed individuare quelle che ci sono sconosciute e quindi potenzialmente … cavalli di Troia.

I sintomi che indicano la presenza di un virus informatico

6. Il browser web con il quale navighiamo ha cambiato grafica

Se negli ultimi giorni notate che la pagina principale del vostro browser è cambiata non sottovalutate questo aspetto.
Quasi sicuramente si tratta di un virus.

Abbiamo elencato solo una minima parte dei sintomi che possono indicare la **presenza di un malware** o di un virus informatico.
Quello che è importante ricordare è che ogni volta che accade qualche cosa di insolito e sospetto sul vostro dispositivo deve farci scattare un allarme e predisporre le azioni correttive di difesa che vedremo in seguito.

Gli strumenti di difesa

La difesa

Gli strumenti

Installare un buon antivirus su PC Windows

Per le esigenze degli utenti comuni, va benissimo l'antivirus **Windows Defender** (l'antivirus di Microsoft incluso "di serie" a partire da Windows 10).
Per le versioni di Windows precedenti alla 10 occorre installare uno degli antivirus gratuiti (**Panda Dome Free** o **Avast Antivirus**).

A prescindere dalla tipologia di antivirus che abbiamo installato, l'importante è che:

- lo si tenga sempre aggiornato, affinché possa individuare le minacce informatiche più recenti
- si eseguano scansioni periodiche del sistema per intercettare potenziali virus che si sono inseriti nel PC

Ricordiamoci di utilizzare l'antivirus per allegati e-mail e chiavette USB sospette!

Gli strumenti

Utilizzare un antivirus sullo smartphone Android

Se si sospetta che il dispositivo **Android** sia infetto da un malware è bene utilizzare un **anti-malware**, effettuando dunque un'apposita **scansione**.

Se non avete un antivirus potete aprire lo store **Google Play** e ricercare "Antivirus Android".

Quelli gratuiti più comuni sono: **Avast Mobile Security** (a pagamento nella versione Premium), **AVG Antivirus** (con banner pubblicitari e a pagamento nella versione Pro), **Bitdefender Antivirus** (rapido, essenziale, a pagamento nella versione Bitdefender Mobile Security).

Gli strumenti

Antivirus per dispositivi Apple

Ma serve davvero un antivirus sui dispositivi Apple? La risposta è **no**.
Allo stesso tempo, **è sbagliato pensare che si tratti di un dispositivo invulnerabile al rischio malware** (del resto sono software progettati con scopi malevoli!).
I sistemi operativi di Apple (per iPhone, iPad, Apple TV) dispongono di misure di sicurezza che rendono meno suscettibili al rischio malware rispetto ad Android.
Ad esempio, le applicazioni si possono installare solo tramite **Apple Store** in cui risiedono solo app certificate da Apple.

Si può affermare che l'iPhone non è invulnerabile ma che il rischio malware è piuttosto limitato se non si effettuano pratiche come il ***jailbreak*** (rimozione volontarie di restrizioni imposte da Apple al proprio sistema).

Gli strumenti

Utilizzare un firewall

E’ un altro modo per proteggere il proprio dispositivo dalle minacce informatiche.
Il Firewall altro non è che un sistema di protezione posto a barriera di due reti (p. es. la nostra rete domestica o il dispositivo Mobile e la rete internet), così da impedire accessi non autorizzati.

Windows Defender (in Windows 10), o applicazioni di ‘firewall’ presenti su Google Play o Apple Store ci vengono utili per questo scopo.

La difesa

Gli strumenti

Mantenere il dispositivo aggiornato

Se vogliamo blindare il dispositivo occorre **mantenere aggiornato il sistema operativo e i programmi installati su di esso**.

Gli aggiornamenti che vengono rilasciati dai produttori (Microsoft, Apple, Google, Huawei) e dai fornitori delle applicazioni spesso contengono correzioni necessarie per impedire a malintenzionati di accedere al PC sfruttando le falle di sicurezza che vengono via via conosciute.

La difesa

Le regole di comportamento

Proteggere il dispositivo con password sicure

Se vogliamo **blindare il dispositivo** è fondamentale **utilizzare delle password sicure** a protezione del sistema e dei file salvati sul disco.

Per quanto riguarda la scelta delle password da utilizzare a protezione del dispositivo e delle registrazioni internet, il consiglio è di usare chiavi d'accesso:

- sufficientemente lunghe (da 8 fino a 12 caratteri)
- difficili da indovinare (quindi prive di senso compiuto)
- composte da numeri, lettere e simboli

Esempi di codifica delle password:

- *salvatoredelmondo96* diventa **$@lvator€delmondo96**
- *seipiùbellodigiuseppe* diventa **6+b€llodig!us€pp€**
- *12345678* diventa **244666668888888**

Le regole di comportamento

Su PC proteggere i file contenenti dati personali con password o crittografia

Per quanto riguarda cartelle e file, la cosa migliore da fare è creare dei **volumi cifrati**, all'interno dei quali andare a inserire tutti i dati da proteggere. Esistono programmi gratuiti, ad esempio **7-Zip**, che rendono il tutto molto semplice (ma non comodissimo in quanto dovremo poi cancellare la cartella non protetta).

Se invece vogliamo proteggere solo alcuni file, per esempio un documento Word o un foglio Excel contenente password di accesso ai vari siti Web su cui ci siamo registrati, ricordiamo che gli strumenti Office permettono di impostare una password di lettura e/o modifica al momento del salvataggio del file.

Le regole di comportamento

Scaricare applicazioni da fonti attendibili

Un altro accorgimento è quello di **scaricare software da fonti attendibili**.
Virus e malware, infatti, spesso vengono scaricati dagli utenti insieme ad applicazioni che apparentemente sembrano innocue.

Prediligere quelle che sono pubblicate negli store Microsoft, Apple, Google dal momento che prima di essere messi a disposizione per il download, vengono sottoposti a processi di analisi e certificazione molto severi.

Quando si scaricano su PC programmi che non sono presenti negli store effettuiamo un controllo con l'antivirus sui file di installazione (.exe, .msi) prima di eseguirli.

La difesa
Le regole di comportamento

Salvare i nostri dati più importanti

Abbiamo visto che fra gli attacchi informatici uno dei più cattivi (ramsonware) è quello che rende inutilizzabili i nostri dati.
In aggiunta a ciò il disco fisso del PC, il PC stesso o il nostro Smartphone potrebbe non funzionare più per cause fisiche e di conseguenza i nostri dati sarebbero inaccessibili.

Per far fronte a questo inconveniente occorre eseguire un salvataggio dei dati su un'altra unità di memoria o usufruendo dei servizi di archiviazione Google o Apple. Fare il **backup dei dati, significa eseguire delle copie dei propri file più importanti** (documenti, foto, video, eccetera).

Farlo **periodicamente** (per es. mensilmente per un utilizzo domestico, dove i dati non sono aggiornati frequentemente) ci consente di recuperarli almeno fino all'ultimo salvataggio.

La difesa
Le regole di comportamento

Evitare le reti Wi-Fi pubbliche

Per quale motivo?
Non essendo adeguatamente protette, le reti Wi-Fi pubbliche possono essere utilizzate abilmente dai criminali informatici per “sniffare” (annusare e carpire) i dati di coloro che vi sono collegati.

Se proprio abbiamo la necessità di connetterci a Internet da PC quando siamo fuori casa, usiamo lo smartphone come modem (hotspot personale); i piani tariffari ci consentono ormai di utilizzare il nostro telefono senza aggravio di costi sul nostro abbonamento.

La difesa

Le regole di comportamento

Registrarsi consapevolmente sui siti web

Come proteggerci:

Limitiamo le registrazioni a siti web affidabili e che presentano politiche di privacy chiare.

Valutiamo i permessi concessi ai siti web prima di confermarli; ad esempio tramite la gestione dei cookie e delle impostazioni di privacy.

Evitiamo di fornire informazioni non necessarie al momento della registrazione.

Usiamo un’email separata per registrarsi a siti e piattaforme secondarie o meno importanti.

Le truffe informatiche più comuni

Le truffe informatiche

Phishing – Cos'è

Il **Phishing** è una pratica che viene eseguita da alcuni truffatori per indurre l'individuo a scrivere i propri dati di accesso ad un servizio, preferibilmente legato ad un conto corrente online; ma potrebbe essere anche un servizio di posta elettronica o social network dove risiedono i propri dati sensibili.

Le truffe informatiche

Phishing – Cos’è

Il **Phishing** viene generalmente attuato mediante l'invio di un'e-mail.
Il truffatore invia una e-mail creata ad arte per invogliare ad aprire un link che si trova all'interno della stessa e-mail.
Il link apre una pagina web **apparentemente** della banca, delle poste o altro servizio online (spedizioniere, supermercato, ecc.).
La pagina è talmente simile a quella originale che non viene colta la differenza; in aggiunta si fa leva sull’**aspetto emotivo ed il carattere di urgenza**; si inseriscono i dati di accesso per entrare sul falso sito e il truffatore se ne impossessa.
Con i dati d'accesso inseriti dal malcapitato il truffatore potrà quindi eseguire operazioni a suo beneficio, rubando soldi e altri dati.

Phishing – Come non cadere nella rete

Prima regola per non cadere nella rete del Phishing è partire dal presupposto, che tutte le email che riceviamo dalla nostra banca o dalle Poste Italiane (o da eBay, o altri servizi riguardanti transazioni economiche o di social network) siano potenzialmente spedite da truffatori.

Seconda regola: **MAI** cliccare sui link proposti dalle email inviate da banche, poste italiane o servizi simili.

Terza regola: se ci colleghiamo alla nostra banca online o alle poste italiane (o servizi simili) utilizziamo sempre l'indirizzo Web originale (che magari abbiamo salvato nei preferiti della app di navigazione)!

Quarta regola: utilizziamo l'autenticazione a due fattori quando possibile.

Le truffe informatiche
Phishing – Esempi

Esistono moltissimi tranelli di phishing:

- ti avvisano che il tuo conto verrà chiuso se non provvedi a collegarti entro ‘**tot**’ ore;
- ti avvisano che hai vinto un premio in denaro o altro e per riceverlo dovrai collegarti "**cliccando qui**";
- ti informano che hai vinto un bonus fedeltà e che dovrai collegarti entro ‘**tot**’ ore per incassarlo;
- ti avvertono che ci sono problemi di sicurezza sul tuo conto e quindi dovrai collegarti per risolverli;
- ti avvertono che c'è stata una transazione non autorizzata e ti chiedono di verificarlo per risolvere la questione;
- ti dicono che hanno limitato l'accesso al tuo conto perché ci sono dei sospetti prelievi sul tuo conto;
- e molto altro!

Le truffe informatiche

Altri tipi di phishing

Phishing telefonico (Vishing)

Non sempre il phishing implica l'utilizzo di un sito web o di mail, le truffe possono arrivare via voce (vishing), con una chiamata da numeri contraffatti che ci chiedono dati o PIN per sbloccare conti o spedizioni.
Anche il canale **Whatsapp** può essere usato per chiedere copie di documenti d'identità che verranno utilizzati per successive truffe.

Phishing tramite SMS

Si chiama **SMishing** l'imbroglio perpetrato tramite SMS.

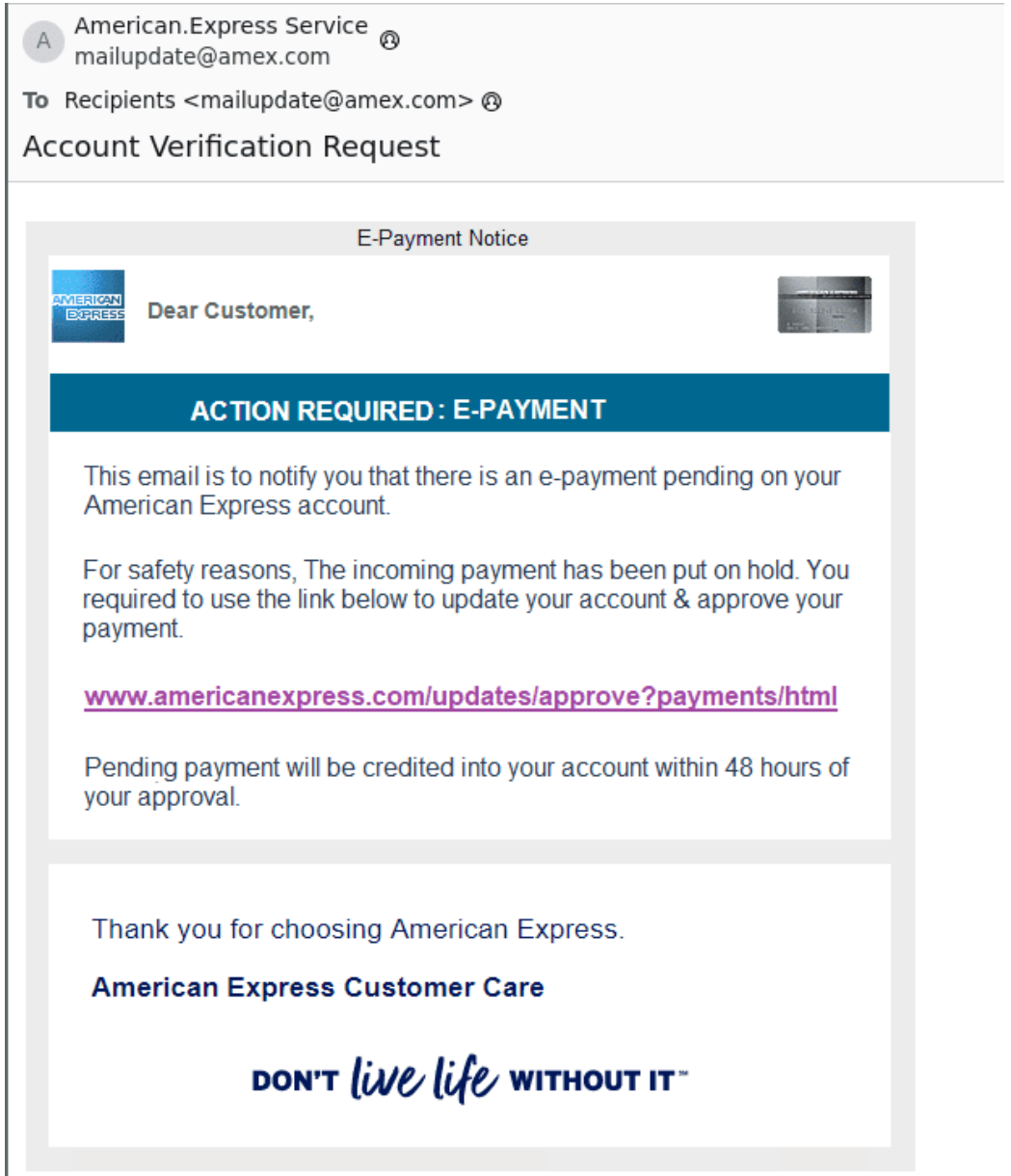
Phishing tramite Codice QR

Con un Codice QR i criminali informatici potrebbero cercare di dirottare l'ignaro utente su un sito appositamente allestito per truffarlo.

La difesa

Phishing – Esempi

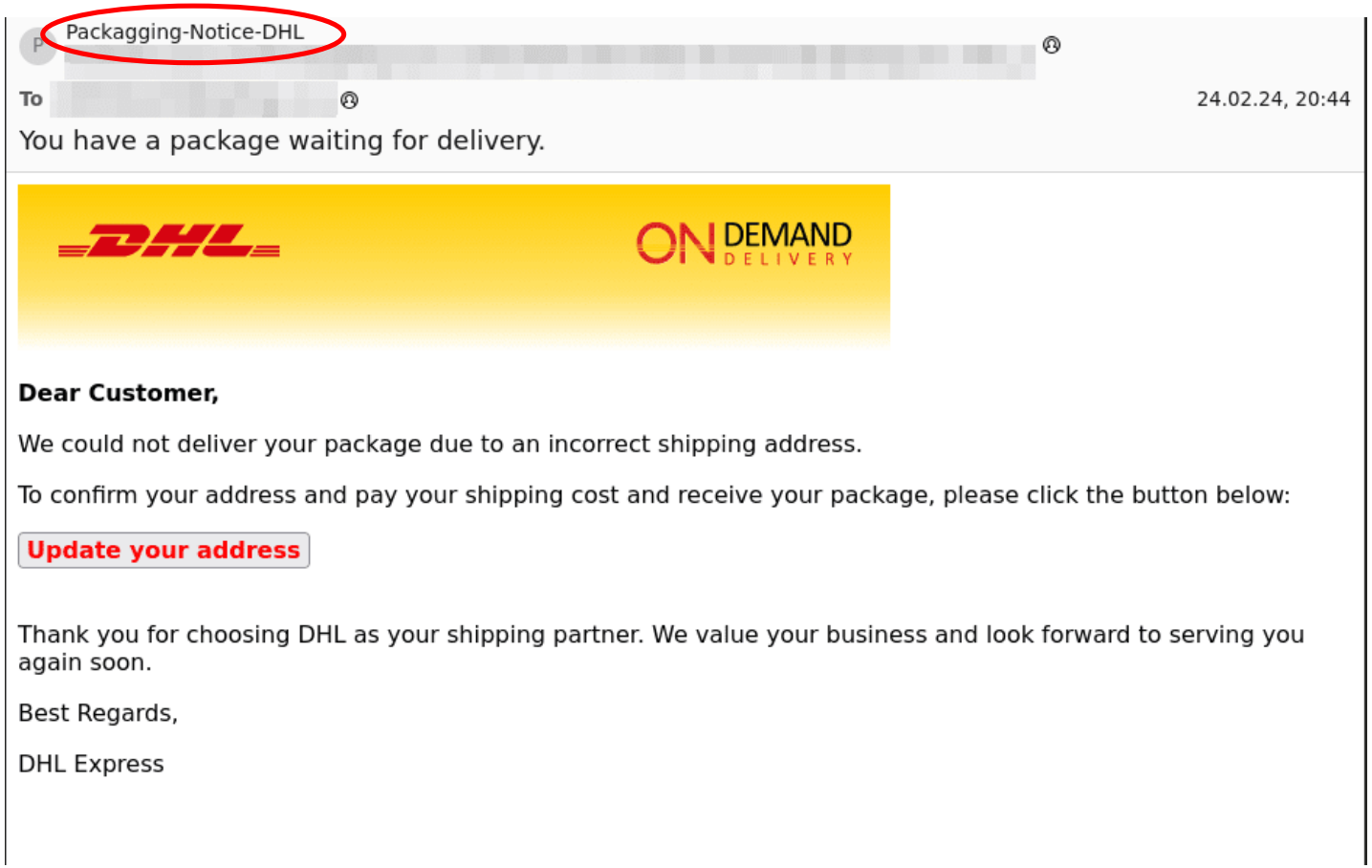
Il link mostrato nell'immagine **non è** quello che un utente incauto aprirà se lo clicca, motivo per cui è importante addestrare gli utenti a passare il mouse sopra i collegamenti sospetti prima di cliccarvi (il che è più facile sui computer che sugli smartphone).



www.americanexpress.com/updates/approve?payments/htm

La difesa

Phishing – Esempi



Packagging-Notice-DHL

To [redacted] 24.02.24, 20:44

You have a package waiting for delivery.

DHL ON DEMAND DELIVERY

Dear Customer,

We could not deliver your package due to an incorrect shipping address.

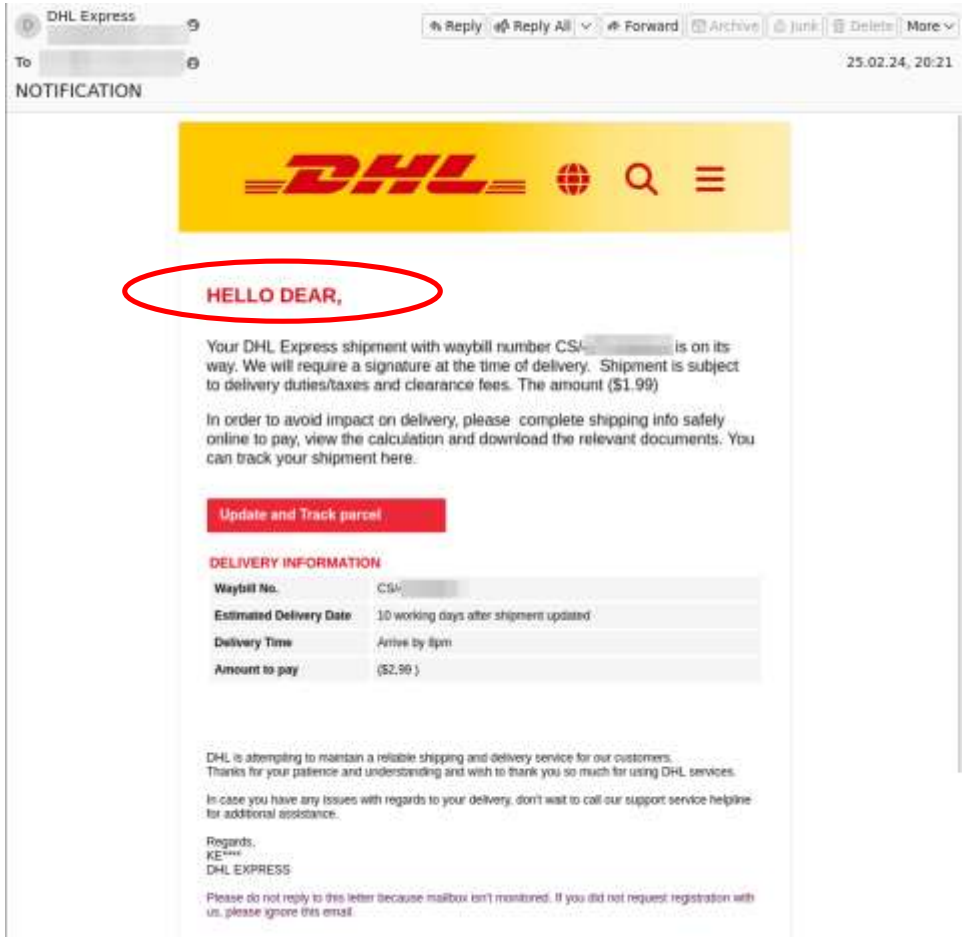
To confirm your address and pay your shipping cost and receive your package, please click the button below:

Update your address

Thank you for choosing DHL as your shipping partner. We value your business and look forward to serving you again soon.

Best Regards,

DHL Express



DHL Express [redacted]

Reply Reply All Forward Archive Junk Delete More

To [redacted] 25.02.24, 20:21

NOTIFICATION

DHL

HELLO DEAR,

Your DHL Express shipment with waybill number CS[redacted] is on its way. We will require a signature at the time of delivery. Shipment is subject to delivery duties/taxes and clearance fees. The amount ($1.99)

In order to avoid impact on delivery, please complete shipping info safely online to pay, view the calculation and download the relevant documents. You can track your shipment here.

Update and Track parcel

DELIVERY INFORMATION

Waybill No.	CS[redacted]
Estimated Delivery Date	10 working days after shipment updated
Delivery Time	Arrive by 8pm
Amount to pay	($2.99)

DHL is attempting to maintain a reliable shipping and delivery service for our customers. Thanks for your patience and understanding and wish to thank you so much for using DHL services.

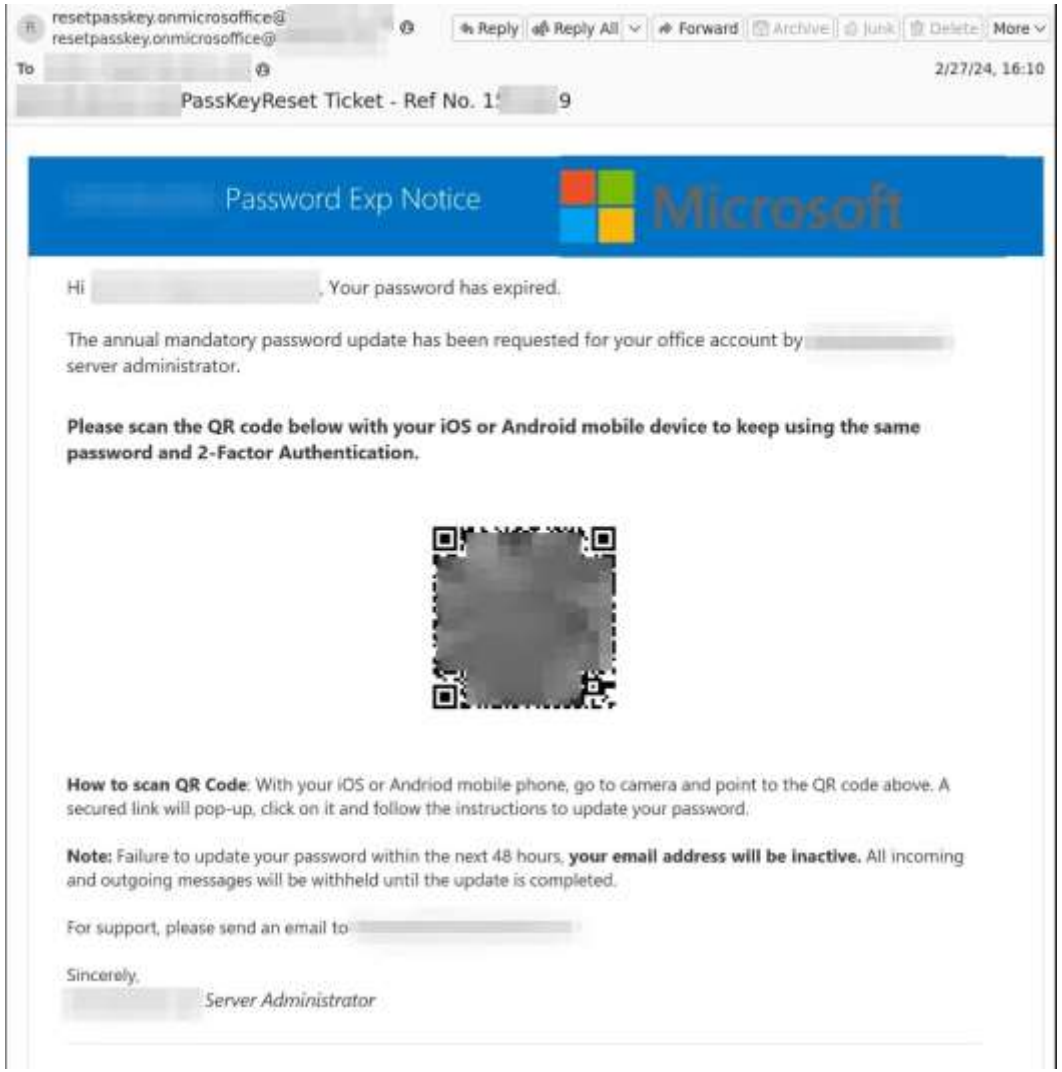
In case you have any issues with regards to your delivery, don't wait to call our support service helpline for additional assistance.

Regards,
KE****
DHL EXPRESS

Please do not reply to this letter because mailbox isn't monitored. If you did not request registration with us, please ignore this email

Notare la parola errata “Packagging” e l’utilizzo di “Hello Dear” come introduzione, improbabile da parte di una compagnia di spedizioni.

Phishing – Esempi



Questo codice QR porta a un sito di phishing in cui la vittima inserisce le proprie credenziali per "aggiornare la propria password", ma invece consegna il proprio nome utente e password affinché i criminali possano utilizzarli in ulteriori attacchi.

Phishing – Esempi

Gentile Cliente,
Un nuovo documento di rendicontazione e a sua disposizione.
Potrete consultarlo e salvarlo sul suo PC entro un anno da oggi, visitando l'area Estratto conto e documentazione del suo Servizi via internet.
Per l'assistenza al Servizi via internet può contattare il numero verde 800.827.455, gratuito anche da cellulare.
Prego di cliccare qui per confermare.
Cordiali saluti.
Servizio Banca di Credito Cooperativo Online.

Questo e un messaggio automatico.
Copyright Banca di Credito Cooperativo S.p.A.

Phishing – Esempio (ACI, hai vinto un kit emergenza)

Esempio di un messaggio ricevuto sulla posta elettronica:

Caro cliente ACI, la tua sicurezza sulla strada è la nostra massima priorità! In segno di ringraziamento per il tuo feedback sulla tua esperienza con ACI, ti offriamo un'opportunità esclusiva per ricevere un kit di emergenza nuovo di zecca per la tua auto. Non perdere questa occasione per essere preparato a qualsiasi situazione imprevista sulla strada.

A seguire un **bottone** contenente un link per richiedere questo fantomatico premio gratuito.
Solitamente queste e-mail sono molto più spoglie e veloci. Invece, qui siamo di fronte ad una cura attenta al testo. Infatti, il messaggio prosegue con **altre informazioni** per convincere l'utente a richiedere il premio.

Le truffe informatiche

Phishing – Esempio (Esselunga e Tupperware)

Ovviamente queste due società non hanno nulla a che fare con questo ennesimo tentativo di raggiro.

Si tratta, ancora una volta, di una **mail phishing**, ossia un messaggio studiato per attirare l'attenzione degli utenti e convincerli ad aprirlo e a fornire i propri dati.

In pratica i cybercriminali inviano una mail in cui si chiede di partecipare a un sondaggio a premi. Chi deciderà di rispondere a una serie di domande, riceverà in regalo un set **Tupperware.** Nella mail si fa menzione anche a un programma fedeltà Esselunga. Basta partecipare a un breve sondaggio online.

Non esiste alcun sondaggio, e non ci sono premi. I malviventi cercano solo il modo di convincere la vittima a cedere i suoi **dati personali,** fra cui quelli della carta di credito.

Le truffe informatiche

Money muling

Il **MONEY MULING** è una pratica finalizzata al **riciclaggio di denaro** proveniente da attività illecite, in particolar modo frodi informatiche e campagne di phishing.

Per riciclare il denaro sporco la criminalità organizzata si serve di persone che sono reclutate con vari espedienti, spesso ignare dell'illegalità delle pratiche, e che vengono chiamate *money mules* (gli "spalloni" di una volta).

L'approccio più comune per le truffe di questo tipo inizia con un **messaggio di posta** che **offre un lavoro facile**, **ben ripagato** e fattibile **da casa** propria.

Se la vittima accetta l'offerta di lavoro, generalmente viene richiesta la disponibilità di operare **trasferimenti di denaro** trattenendo una commissione: il denaro che verrà trasferito proviene da attività illegali, facendo così ricadere l'operazione nel **reato di riciclaggio**.

Riassumendo…….

GRAZIE PER L'ATTENZIONE

Ci rivediamo il 30 Gennaio.
Parleremo di:

Il monopolio del software nell'informatica ed il suo superamento

Quali vantaggi per noi?