28 MAGGIO 2020

CyberSecurity e HR Management

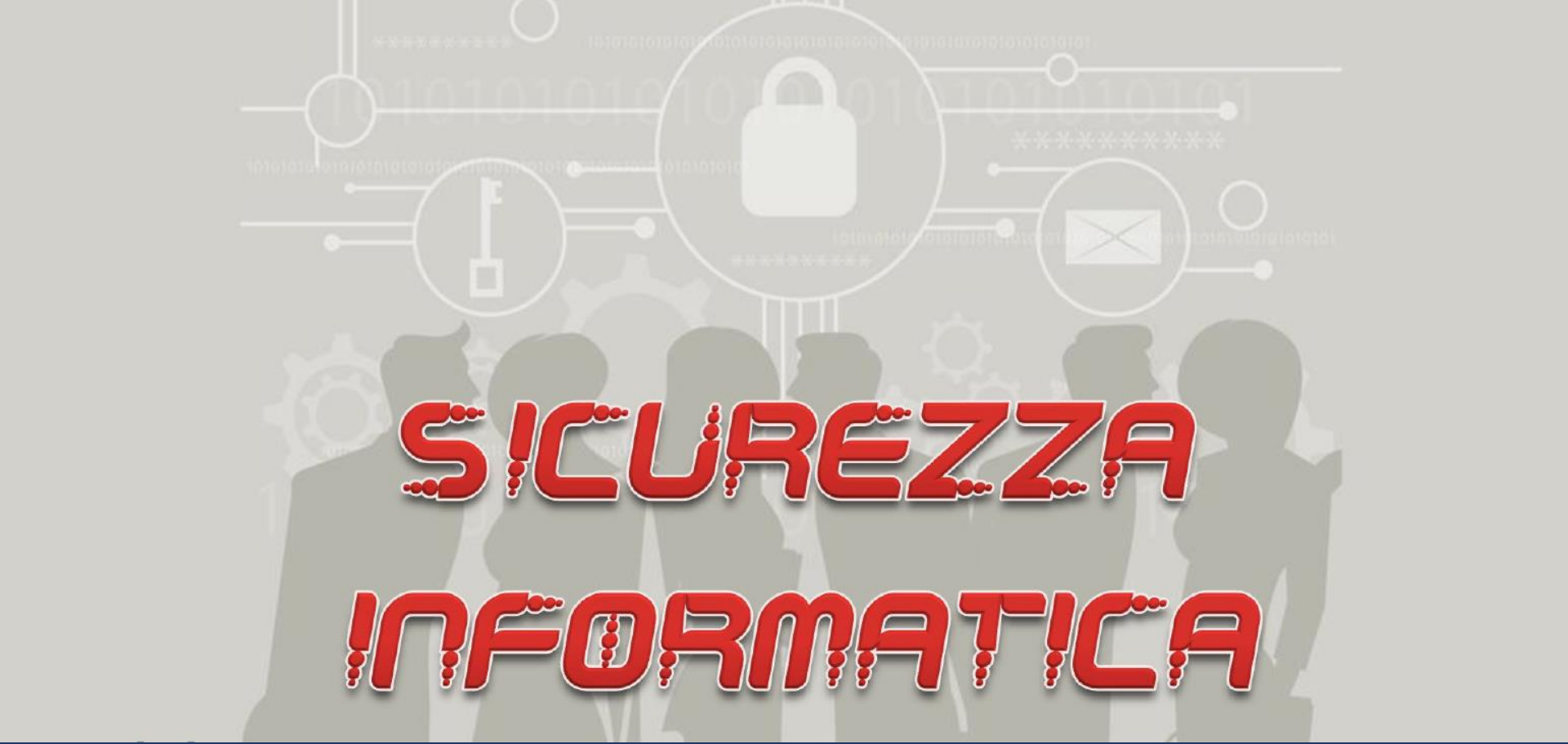
L'antivirus più efficace sta seduto davanti al computer

Free Webinar

Relatori
Cristina Sartori – Direttore Business Unit Investigazioni
Roberto Grigoletto – Consulente CyberSecurity

YALI CONSULTING

abbrevia
INDAGO ERGO SOLVO



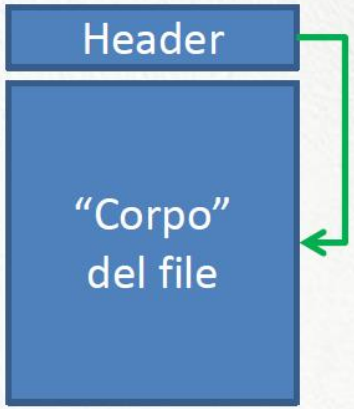
abbrevia
INVESTIGAZIONI

abbrevia
INVESTIGAZIONI

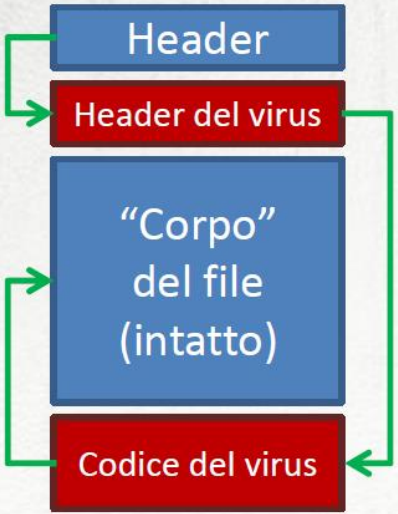
I Virus: cosa sono e come funzionano?

I virus veri e propri infettano solo i programmi.

Programma sano



Programma infetto



I Virus: i “ransomware”

Il nome “ransomware” deriva da “ransom”:
ricatto in inglese.

Criptano (codificano) tutti i files dell’utente e
richiedono un pagamento per “sbloccarli”.

Inizialmente esistevano modi per sbloccarli: software,
servizi (NSA), pagando.

Ora ci sono troppe tipologie e gli hacker si sono fatti
“avidi”. Se ci colpisce un ransomware l’unica salvezza
è un backup precedente.

I Virus: come si combattono?

Munirsi di un buon antivirus, anche gratuito.


Microsoft Defender


Avast


AVG

Mai più di un antivirus sullo stesso PC

Nessun antivirus riconosce TUTTI i virus, quindi:
PRUDENZA!

Quali sono le altre minacce?

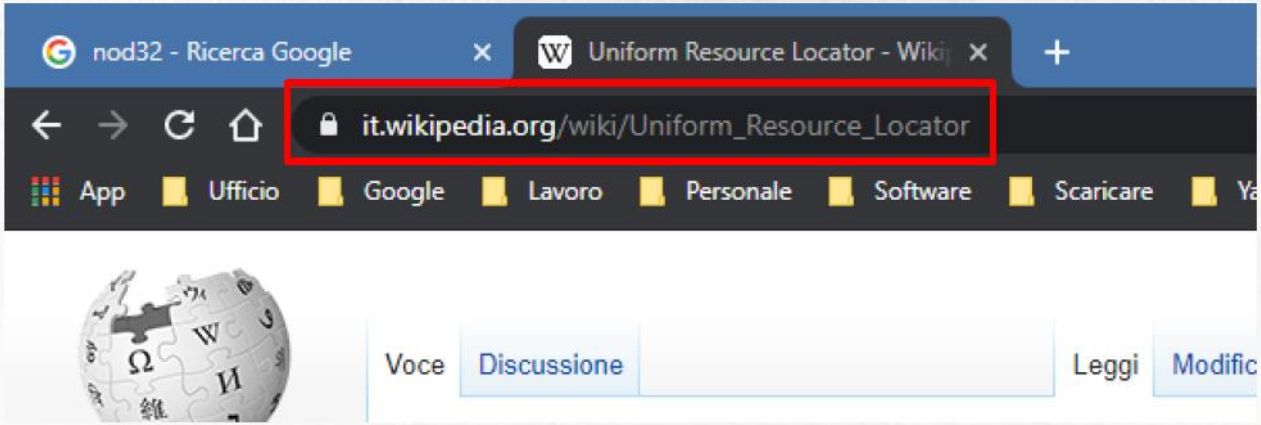
- Siti internet pericolosi
- Phishing (richiesta informazioni)
- Ingegneria sociale (inganni e truffe)

Script: “programmi” di solo testo non rilevabili da nessun antivirus

abbrevia
INVESTIGAZIONI

URL: cosa sono?

URL: Uniform Resource Locator (indirizzo internet)



URL: come capirli?

Sicurezza SSL

Dominio del sito

https://www.miosito.com/cartella/pagina.htm

SSL significa che la comunicazione è criptata.
NON significa che il sito è autentico!

Se fornite informazioni personali, SSL è indispensabile!

Un sito senza SSL non è automaticamente pericoloso.

SSL può essere indicato dal lucchetto: 

abbrevia
INVESTIGAZIONI

Link: cosa sono?

I link sono delle scritte “cliccabili” che
ci mandano a un URL.

http://www.google.it
Clicca qui per andare su Google

I link possono essere in un sito, in un documento, in una mail, in un messaggio, etc.

I link non sono “virus”, quindi l’antivirus
non può proteggerci!

Link: a cosa puntano davvero?

La “scritta” di un link non è necessariamente il sito a cui ci manda!

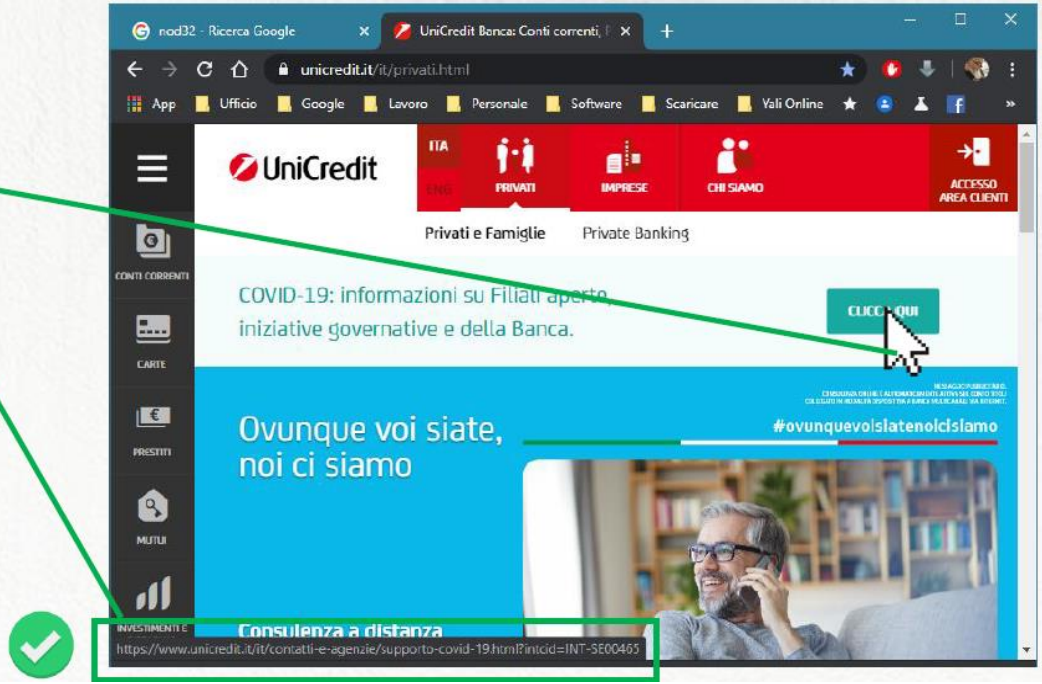
E’ tecnica comune creare un link dall’aspetto “innocuo” e farlo puntare a un sito malevolo.

Dobbiamo imparare a capire dove puntano i link.

Link: a cosa puntano davvero?
Su internet

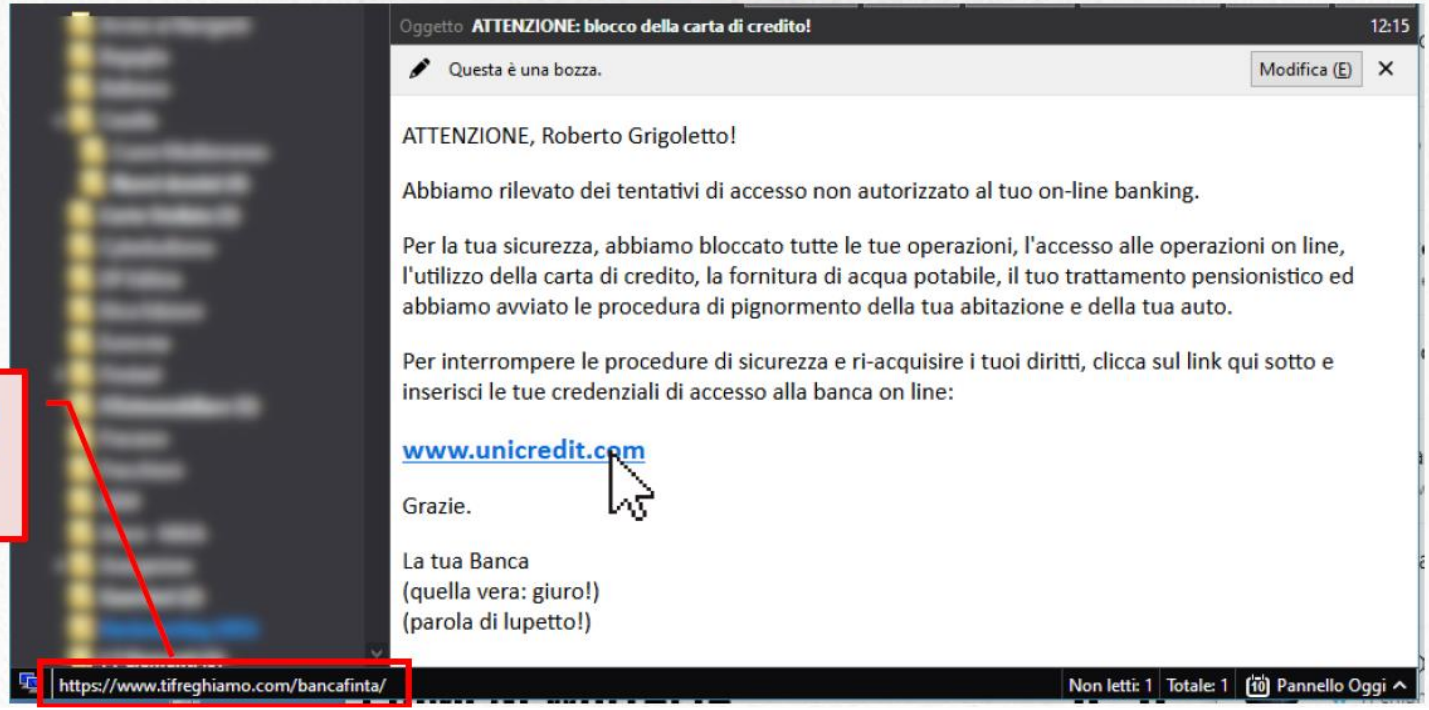
Mouse in “hovering”: sopra il link senza cliccare

Vero indirizzo a cui punta il link



abbrevia INVESTIGAZIONI

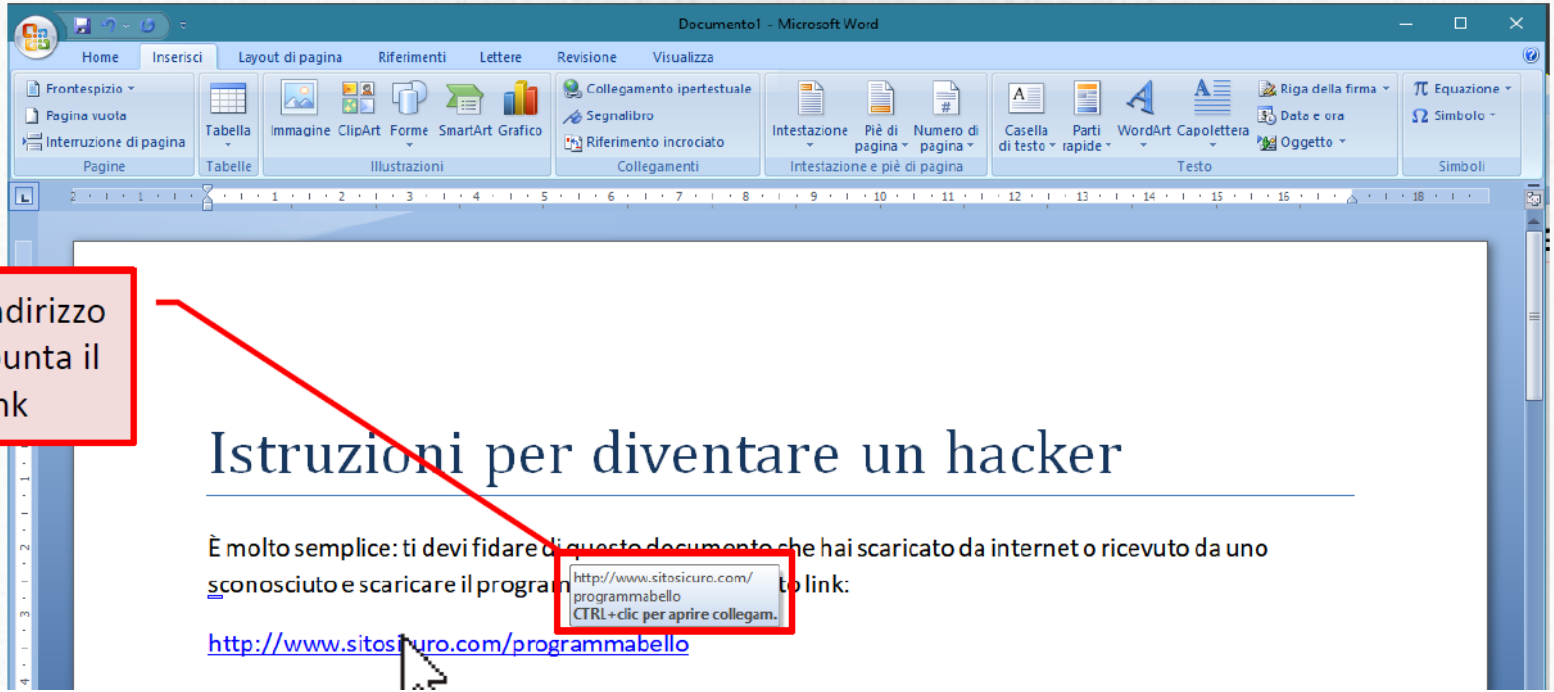
Link: a cosa puntano davvero?
Nelle mail



Vero indirizzo a cui punta il link

abbrevia
INVESTIGAZIONI

Link: a cosa puntano davvero?
Nei documenti



Vero indirizzo a cui punta il link

abbrevia INVESTIGAZIONI

LE EMAIL

abbrevia
INVESTIGAZIONI

Mail: come gestirle?

Cosa si può fare?

- Ricevere una mail non ci infetta
- Aprire un mail non ci infetta
- Leggere una mail non ci infetta
- Rispondere a / inoltrare una mail non ci infetta
- Salvare un allegato non ci infetta

Mail: come gestirle?

Cosa è pericoloso:

- Cliccare sui link, pulsanti e altro.

- Aprire allegati sconosciuti

- Eseguire istruzioni dubbie

La “PEC”: è sicura?

Il sistema “PEC” (Posta Elettronica Certificata) serve solo ed esclusivamente a certificare “giuridicamente” l’invio, la ricezione e la lettura di una mail. Nient’altro.

La “PEC” non fornisce alcun tipo di protezione contro virus e script.

Alcune “PEC” impediscono la ricezione di posta da caselle che non sono “PEC” esse stesse.

Per quanto per un hacker sia un po’ più complicato inviarvi una mail da “PEC” a “PEC”, la cosa è assolutamente fattibile.

Ai fini della sicurezza, una “PEC” deve essere trattata esattamente come una normalissima mail.

Truffe, scam e mail false

Il mittente di una mail può facilmente essere falsificato anche senza “craccare” la mail del mittente stesso.

Se una mail è “strana” o “inaspettata”, non fidarsi anche se arriva da un mittente “fidato”: potrebbe non essere lui.

Nel caso di mail sospette, procedere sempre al “precontatto” prima di aprire qualsiasi allegato o cliccare su un link.

Ricatti, hacking e altri mostri

Girano molte mail che – pur non contenendo “virus”
o “script” – sono estremamente pericolose.

Parliamo delle mail di ricatto, di minaccia, di sanzione (finta),
di ingiunzione (finta), etc.

Sono vere? Come distinguerle? Come difendersi?

Ricatti, hacking e altri mostri
I ricatti vari

La loro tecnica è quella di “sparare nel mucchio”.

Per quanto queste mail possano spaventare, non è economicamente vantaggioso per un hacker “impossessarsi” in modo così completo di un PC da remoto.

Prestate attenzione al “materiale” che dicono di possedere: se anche solo una cosa è falsa, è falso tutto!

Vale la regola: male non fare, paura non avere. ;-)

Per sicurezza e paranoia, potete sempre mettere un pezzetto di nastro rimovibile sulla webcam.

In 29 anni di attività, non ne ho mai rilevata una vera.

Ricatti, hacking e altri mostri
Sanzioni, blocchi e “multe”

Il computer si blocca e compare una scritta:
“Questo computer ha svolto attività illegali ed è stato bloccato
È in corso un’indagine penale la cui conseguenza può
essere l’arresto e la detenzione.
Per evitare di incorrere in un processo penale, procedere
al pagamento della sanzione di xxx.xx € con il metodo indicato
entro X giorni.”

Semplice: nessun organo ufficiale dello stato procede in questo modo nelle indagini di reati informatici di qualsiasi tipo ed entità.
È SEMPRE una truffa.

ALLEGATI E FILES

abbrevia
INVESTIGAZIONI

Riconoscere files e allegati

Windows riconosce i files basandosi sull'"estensione".

L'estensione sono gli ultimi caratteri del nome di un file (dopo un punto):

documento.**doc**, fattura.**pdf**, contabilità.**xlsx**, programma.**exe**, immagine.**jpg**, programma.**com**, script.**js**

Attenzione alle doppie estensioni: "documento.pdf.exe"
L'estensione che "conta" è sempre l'ultima!

Normalmente, le estensioni non sono visibili (servono solo al sistema).

L'icona di un file NON è un elemento di riconoscimento: può essere modificata!

Riconoscere files e allegati
Quali devo evitare?

.**exe**: Eseguibile. È un programma.

.**com**: Command. È un programma.

.**cmd**: Command. È un programma.

.**bat**: Batch. È un programma.

.**js**: Java Script. È un programma.

.**scr**: Script. È un programma.

.**ws**: Windows Script. È un programma.

.**html/htm**: Codice HTML. Può contenere script. (pericoloso se in allegato a una mail)

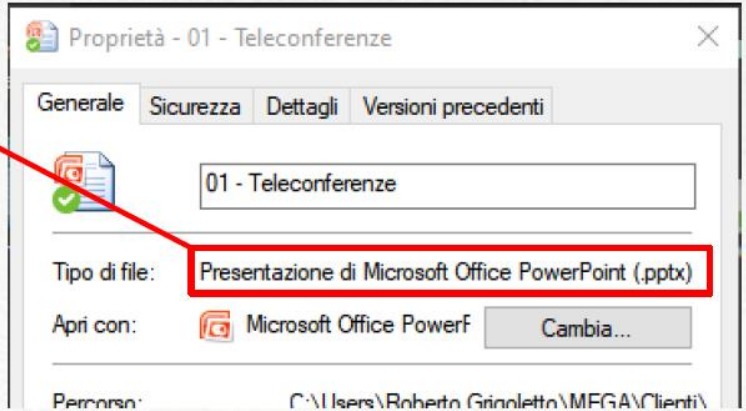
L'antivirus non vi può proteggere!

.**zip/rar/7z**: Achivio compresso. Non è pericoloso in sé, ma bisogna prestare attenzione a cosa contiene!

Riconoscere files e allegati
Nel sistema

Windows nasconde le estensioni dei files,
ma noi possiamo visualizzarle:
Click con il pulsante destro del mouse sul file
Click su “Proprietà”

Tipo del file

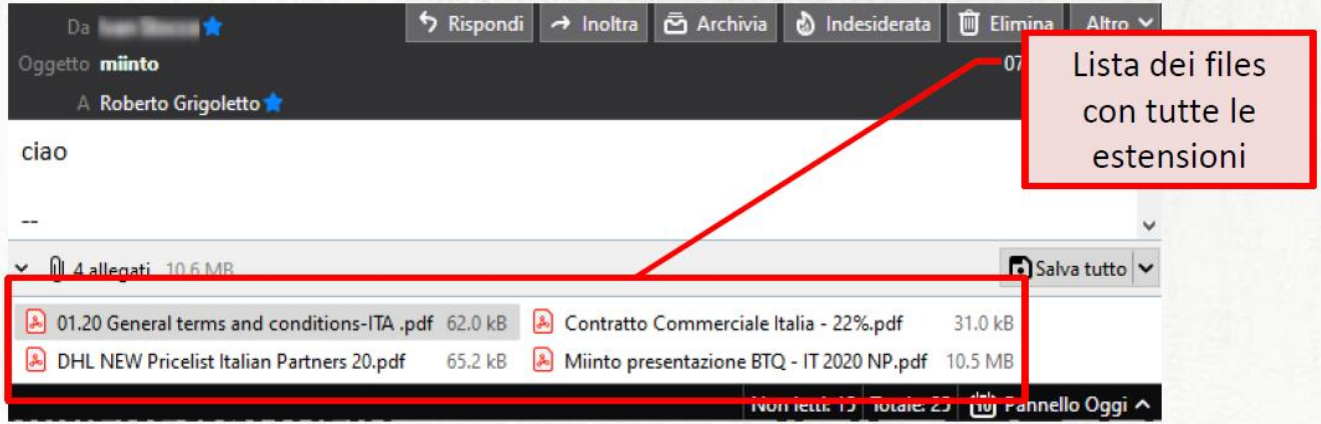


Riconoscere files e allegati
In internet

Quando su internet scarichiamo un file,
lo facciamo tramite un link.
Quindi è sufficiente seguire i consigli visti per i link
e identificare l'estensione nel link:

Riconoscere files e allegati
Nelle mail

Fortunatamente, i programmi di posta non nascondono le estensioni degli allegati mail: basta leggerle.



abbrevia INVESTIGAZIONI

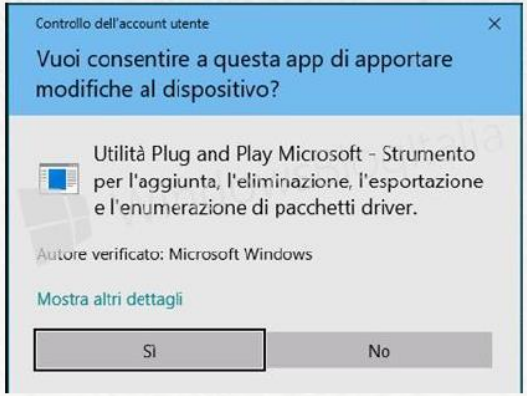
abbrevia
INVESTIGAZIONI

Le autorizzazioni di sistema

Praticamente tutti i sistemi operativi moderni (da Windows 7 in poi) ci presentano una richiesta di autorizzazione ogni volta che un programma tenta di modificare il sistema stesso:

Le autorizzazioni di sistema

Occorre sempre prestare attenzione: se stiamo installando un programma o un aggiornamento, è normale. Se stiamo visitando un sito o aprendo un allegato è un importantissimo campanello d'allarme!



IL BACKUP

abbrevia
INVESTIGAZIONI

Il backup: perché farlo?

Il backup è l'unico sistema che ci può proteggere da:

1) Un attacco ransomware.

2) Un guasto grave del PC (disco fisso)

3) Un grave errore del'utente.

4) Qualsiasi situazione in cui siano stati compromessi i nostri dati.

Il backup “incrementale”: come funziona?

Il backup incrementale “salva” i dati in modo particolare e risparmia spazio:

1) Una prima copia viene effettuata completa.

2) Altre “x” copie vengono effettuate copiando solo i files modificati dalla data del’ultimo backup completo (punto 1)

3) Ogni “X” copie ne viene effettuata nuovamente una completa.

4) In questo modo si può tenere uno “storico” dei file del computer anche molto “lungo” risparmiando molto spazio e tenendo più copie (a vari stadi di lavorazione) di ogni file.

Il backup “incrementale”: perchè?

1) Ci fa risparmiare spazio.

2) Permette di tenere uno storico più vasto.

3) Non sempre ci accorgiamo subito di essere stati attaccati da un virus. Se ce ne accorgiamo dopo aver fatto un backup non incrementale, anche il backup sarà infetto, quindi inutile. Con il backup incrementale possiamo risalire a come erano i files prima dell’attacco anche se ce ne accorgiamo tardi.

Il backup su disco fisso esterno

Non ha senso fare un backup sullo stesso disco di sistema o su un disco interno dello stesso PC:

1) Non ci protegge dai ransomware e da altri virus.

2) Non ci protegge dai guasti hardware.

3) Non ci protegge dai furti.

Per questi ed altri motivi, il backup deve sempre essere effettuato su un disco esterno, che deve essere collegato al PC per il solo tempo necessario al backup. Collegato prima e scollegato dopo.

LE REGOLE

abbrevia
INVESTIGAZIONI

La difesa: le regole d'oro

1) Dovete sapere (segnarvi) tutte le vostre password. Un utente che non conosce le proprie password è come una persona che non ha le chiavi della propria casa.

2) Se una mail è inaspettata o strana, contattate sempre il mittente tramite un diverso canale per una conferma.

3) Verificate sempre i link con il metodo dell'"hovering" con il mouse prima di cliccare.

4) Prima di aprire un allegato inatteso controllate sempre l'estensione con uno dei metodi indicati

5) Se sospettate di essere stati attaccati/infettati, non perdete tempo e modificate (o chiedete di modificare) immediatamente tutte le vostre password.

6) Non esitate mai a chiedere il parere di un tecnico in ogni situazione dubbia.

7) Se il vostro PC presenta segni di infezione evidenti, spegnetelo immediatamente e contattate un tecnico senza accenderlo più.

La difesa: la regola di platino

Fretta, panico e distrazione fanno più danni di qualsiasi virus!

Grazie per la partecipazione

abbrevia
INVESTIGAZIONI

Cristina Sartori
Direttore B.U. Investigazioni
Mob. + 39 393 9692701
Mail c.sartori@abbrevia.it