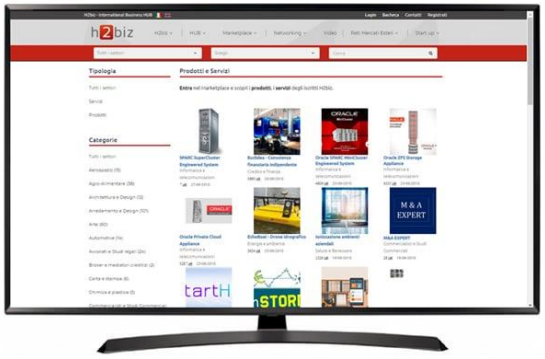
Lavoro realizzato, su commissione dell'Unione Nazionale Consumatori di Basilicata, nell'ambito del progetto pilota sperimentale "Digitalmentis" educazione digitale dei consumatori adulti. Iniziative a vantaggio dei consumatori, linea d'intervento art. 6 comma 1, D.M 10.08.2020 e dell'art. 3 comma 1 del D.M 6.05.2022.

Dott. Roberto Fantini

SICUREZZA INFORMATICA
Non solo PC…

Una volta era solo il PC…

Adesso abbiamo un e-commerce…



Siamo presente su diversi marketplace…

E facciamo tante videoconferenze…

Perché i nonni e gli anziani finiscono spesso vittime di truffe e frodi creditizie

- I motivi principali per cui nonni e genitori vengono presi di mira dai cybercriminali sono due:
- **tendono ad avere più risparmi dei giovani**, così come dei gioielli e altri oggetti di valore.
- possono più facilmente cadere vittima delle truffe "**a bassa tecnologia**" che non richiedono grosse competenze tecniche da parte dei truffatori. Un esempio di truffa a bassa tecnologia? Le truffe telefoniche agli anziani: i criminali possono facilmente informarsi in rete, ad esempio sui social media, a proposito della famiglia della persona anziana presa di mira. Possono scoprire che un nipote lavora all'estero, trovarne nome e cognome e altre informazioni preziose (il nome della moglie, o della fidanzata) e poi chiamare la vittima convincendola a inviare del denaro per aiutare il nipote, finito in guai economici o con la giustizia.

Sicurezza online per nonni e genitori: come aiutarli

- Ecco ora alcuni consigli che possiamo dare ai nostri nonni e alle persone meno giovani per non finire nelle trappole dei cybercriminali:
- **Creare delle password complesse**. Spesso non comprendiamo appieno l'importanza della password, che è la chiave che protegge la nostra identità (e i nostri soldi!) in rete. Se utilizziamo, ad esempio, la nostra data di nascita, è come avere una serratura che può essere aperta con un passepartout.
- **Non comunicare o condividere informazioni finanziarie** (come i dati della carta di credito o del documento d'identità, o il proprio IBAN) via e-mail, SMS o app di messaggistica, a nessuno.

Perché i nonni e gli anziani finiscono spesso vittime di truffe e frodi creditizie

•**Non fidarsi** di chi ci contatta dicendo di parlare a nome di un familiare, un amico o anche la nostra banca o un'azienda che conosciamo.
Parlare sempre direttamente con la persona o azienda interessata contattandola noi tramite numeri di telefono che già conosciamo o che
•comunque sono ufficiali.
•**Non pubblicare sui social informazioni sulle proprie abitudini**.
Questa è una delle vulnerabilità più sfruttate in caso di truffe romantiche.
Il truffatore o la truffatrice dicono di averci visti nel bar che, guarda caso, diciamo su Facebook di frequentare ogni giorno per colazione,
e così inizia una conversazione che prosegue in un corteggiamento,
e si conclude con una richiesta di denaro.

- **Navigare in sicurezza nell’era digitale**
- Con l’aumento della digitalizzazione, anche coloro che non sono grandi fan dei computer si trovano a doverli utilizzare per svariate ragioni. Gli anziani, in particolare, possono sentirsi sopraffatti dalla nuova tecnologia. In termini di sicurezza, può sembrare che ci sia molto da fare per mantenere dati e dispositivi al sicuro. È importante conoscere le minacce e come proteggersi.
- **1. Evitare di cliccare su link sospetti**
- Non cliccare su link che chiedono di compilare informazioni personali. Banche e altre istituzioni finanziarie non inviano email con link, specialmente se questi link richiedono l’aggiornamento delle informazioni personali. Se un sito web promette qualcosa in cambio dell’inserimento dei dati personali, è probabile che si tratti di phishing.
- **2**

- **Diffidare delle offerte troppo belle per essere vere**
- **Se viene offerto un servizio, prodotto o gioco gratuitamente e non è chiaro come i produttori stiano guadagnando, è meglio evitarlo. Potrebbe comportare la visione di pubblicità invasive, acquisti in-app o ricezione di email di marketing.**

- **Non credere a pop-up e chiamate che segnalano infezioni**
- Non credere alle chiamate non richieste e ai siti web che affermano che il computer è infetto. Questi sono noti come truffe di supporto tecnico. Solo le piattaforme di sicurezza possono rilevare un’infezione.
- **4. Evitare il download di programmi che si definiscono ottimizzatori di sistema**
- Questi software, inclusi aggiornatori di driver e pulitori di registro, sono spesso programmi potenzialmente indesiderati che non offrono alcun beneficio reale e possono comportare rischi

- **Disabilitare le notifiche web push**
- Queste notifiche sono raramente utili per l’utente e sono spesso utilizzate per ingegneria sociale e pubblicità invadente.
- **6. Mantenere il browser aggiornato**
- È importante applicare gli aggiornamenti dei browser il prima possibile per proteggere contro le vulnerabilità.
- **7. Cercare HTTPS e il simbolo del lucchetto**
- La presenza di un lucchetto accanto alla barra degli indirizzi indica che il traffico tra il computer e il sito web è crittografato.

- **8. Utilizzare l’autenticazione multi-fattore**
- L’uso dell’autenticazione multi-fattore aumenta la sicurezza richiedendo un ulteriore livello di verifica oltre alla password.
- **9. Utilizzare un gestore di password**
- I gestori di password aiutano a creare e ricordare password sicure e non inseriscono automaticamente le password nei siti falsi, aiutando a identificare i tentativi di phishing. Questo passaggio potrebbe richiedere tempo e l’aiuto di qualcuno con maggiore competenza tecnica, ma aumenta notevolmente la sicurezza a lungo termine.

I RISCHI DELLA RETE
Attenzione ai «crackers»

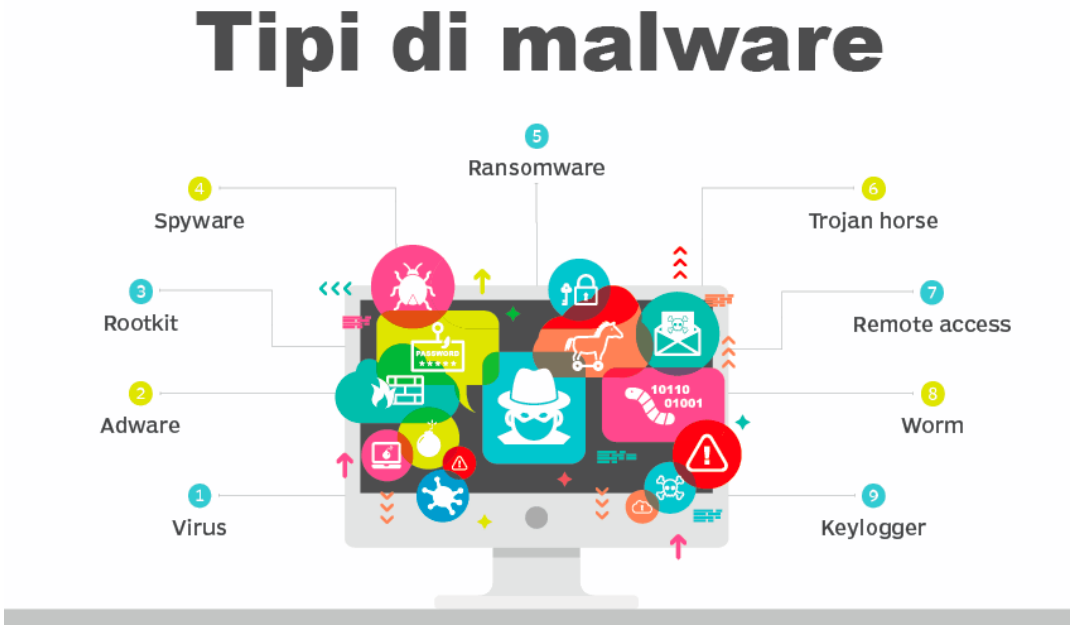
- **Hacker**: esperto informatico che usa le sue competenze per creare nuovi software e che si può anche introdurre in reti informatiche, ma con l'unico scopo di dimostrare quanto sia bravo a "violare" i sistemi di sicurezza, segnalando i problemi a chi ne è proprietario. È come se una persona vedesse una porta corazzata che protegge una gioielleria, la aprisse grazie alla sua destrezza e poi lasciasse un bigliettino indicando i problemi che aveva la porta ma non toccasse nessun gioiello.

- **Cracker**: è sempre un esperto informatico, solo che è un criminale. Dunque viola reti e sistemi informatici con l'unico scopo di rubare dati e informazioni, o creare nuovi software tipo virus. Quindi apre la porta corazzata della gioielleria per rubare i gioielli.

I PERICOLI CHE ARRIVANO AL PC
Malware

Un *malware* è un qualsiasi software creato con il solo scopo di creare danni più o meno estesi al computer su cui viene eseguito.

Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio".



I PERICOLI CHE ARRIVANO AL PC
Trojan

Un *trojan*, (Cavallo di Troia), è un programma per computer che contiene funzionalità maliziose note a chi lo ha programmato, ma non all'utente.

Un *trojan horse* è chiamato in questo modo poiché esegue delle azioni nascoste all'utente, facendo credere a quest'ultimo di essere in possesso di qualcosa di realmente utile. Dunque abbiamo 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dal pirata per inviare istruzioni che il server esegue.

I PERICOLI CHE ARRIVANO AL PC
Worm

Un *worm* è una particolare categoria di *malware* in grado di autoreplicarsi.

Tipicamente un worm modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. Il worm tenta di replicarsi sfruttando Internet

I PERICOLI CHE ARRIVANO AL PC
Spyware

Mentre state navigando in Internet, qualcuno, di nascosto, sta raccogliendo dei dati sul vostro Pc.
Si tratta di un programma "*Spyware*". Vengono usati da "*spamer*" e "*craker*" ovvero diversi tipi di pirati informatici, e anche da società che si occupano di pubblicità on-line, per conoscere le vostre abitudini quando navigate in Internet, quali programmi usate e quali avete installato. Alcuni raccolgono dati anche su tutto quello che digitate.

I PERICOLI CHE ARRIVANO AL PC
Phishing

Il *phishing* è una tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli, opportunamente creati per apparire autentici.

Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati sensibili, come numero di conto corrente, nome utente e password, numero di carta di credito ecc.

Per difendersi dal *phishing* inviato via e-mail, basta cancellare l'e-mail.

I PERICOLI CHE ARRIVANO AL PC
Adware

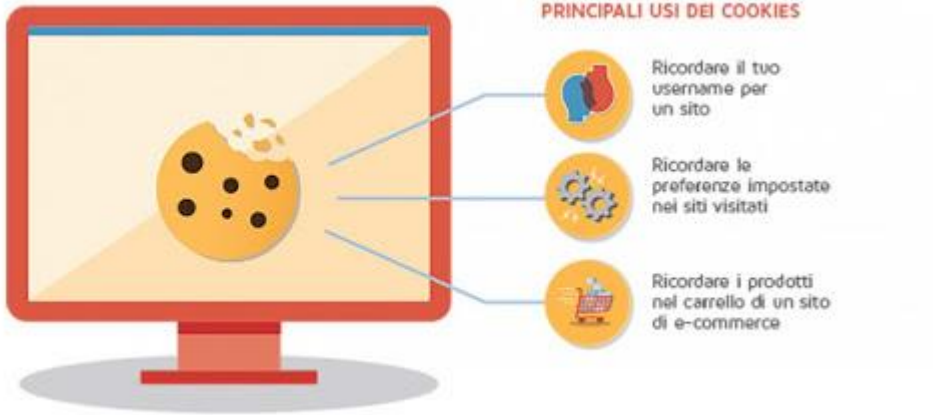
E’ un tipo di software distribuito gratuitamente in cambio della visualizzazione di pubblicità tramite appositi banner inseriti nel programma stesso. È’ una forma di distribuzione che si è diffusa notevolmente grazie a Internet e un modo per ripagare dei costi di sviluppo i produttori di programmi. Spesso viene data la possibilità di far scomparire il banner dalla finestra di lavoro del programma, pagando una piccola cifra in denaro al produttore, di entità simile a quelle richieste per la fornitura di software in modalità shareware.

I PERICOLI CHE ARRIVANO AL PC
Hijacking

Hijacking: portare l'utente a visitare determinate pagine indipendentemente dalla sua volontà e dalle sue abitudini in rete. Questo può essere fatto solo assumendo direttamente il controllo della macchina usata dall'utente.
Questa tecnica permette ai dirottatori di eseguire sul nostro computer una serie di modifiche tali da garantirsi la nostra visita alle loro pagine al solo scopo di incrementare in modo artificioso il numero di accessi e di click diretti al sito e conseguentemente incrementare i guadagni dovuti alle inserzioni pubblicitarie.
Queste azioni possono limitarsi alla semplice modifica della pagina iniziale del browser, all'aggiunta automatica di siti tra i preferiti fino a radicali modifiche al nostro

I PERICOLI CHE ARRIVANO AL PC
Cookie

I *cookies* (letteralmente "biscottini") sono piccoli file che i siti web utilizzano per immagazzinare alcune informazioni nel computer dell'utente. I *cookie* vengono inviati dal sito web e memorizzati sul computer. Sono quindi re-inviati al sito web al momento delle visite successive. Le informazioni all'interno dei *cookie* sono spesso codificate e non comprensibili.
Le applicazioni più comuni vanno dalla memorizzazione di informazioni sulle abilitazioni dell'utente, alla tracciatura dei movimenti dell'utente stesso all'interno dei siti web che visita.

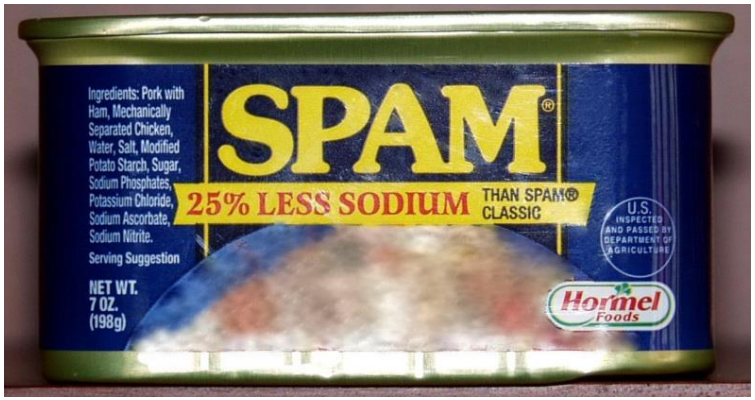


I PERICOLI CHE ARRIVANO AL PC
Spam

Lo spam (o e-mail spazzatura) è l'invio di messaggi indesiderati (generalmente commerciali) che invadono le caselle di posta elettronica.

Gli spam arrivano al vostro indirizzo grazie a programmi specifici che sfruttano tutto ciò che contiene una “@” nei forum, blog, siti web e nelle chat. Questi programmi, chiamati crawler, funzionano grosso modo come i motori di ricerca in internet.

Il rimedio è quello di far controllare le e-mail da un programma che fa da filtro antispam.



VIDEOCONFERENZE
Problemi organizzatore

Quando compriamo e paghiamo un corso on-line ai problemi di un sito di e-commerce, si aggiungono i problemi di sicurezza durante la lezione. Se usiamo piattaforme non sicure si rischia che possano “intrufolarsi” persone non desiderate (potrebbero entrare gratis oppure sabotare la lezione).

Ai primi di aprile 2020 la famosa piattaforma di videoconferenza ZOOM, tra le più utilizzate in questo periodo, ha subito un attacco informatico in cui sono stati rubati oltre 500mila credenziali di utenti, che sono stati posti in vendita a costi bassissimi nel “dark web” (zona del web il cui accesso avviene non con motori di ricerca ma con software e browser specifici e dove si trovano informazioni illegali riguardanti droga, armi, materiale pedopornografico, identità rubate, ecc.).

Videochat, Zoom ancora sotto attacco: oltre 500 mila credenziali finiscono sul dark web

19 aprile 2020

Sono state messe in vendita per pochi centesimi o addirittura rilasciate gratis. La società dell'app diventata popolarissima in tempo di quarantena per coronavirus invita i suoi utenti a cambiare password

VIDEOCONFERENZE
Problemi utente

Fate attenzione a chi è l'organizzatore e quale piattaforma usa. Se poi si partecipa a corsi gratuiti, ricordatevi che nulla è gratis ed il prezzo che pagate sono i dati che lasciate. Si consiglia di aprire una casella email da utilizzare per registrarsi in tutte le attività gratuite che trovate in rete in modo da usarla come "contenitore" di tutto lo spam che poi puntualmente vi arriverà.

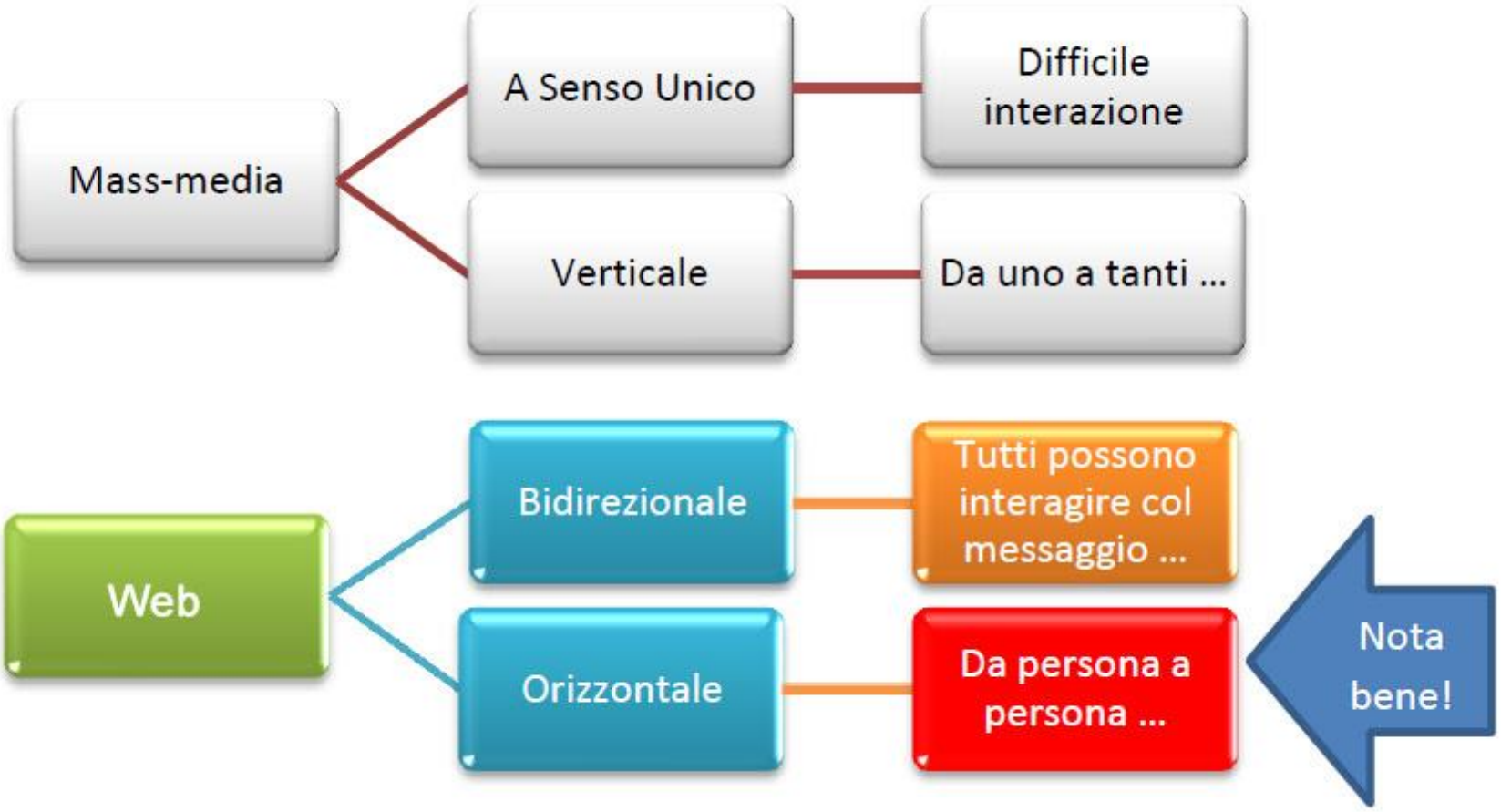
Sì, è vero che esiste un fantomatico Regolamento Generale sulla Protezione dei Dati (GDPR) a tutela della privacy a cui si devono attenere i siti web e i gestori di dati sensibili, ma è la norma più violata da tutti.

VIDEOCONFERENZE
Riunioni online

La sicurezza della piattaforma da usare è fondamentale. Si rischia che durante una riunione, nella quale ci si scambia informazioni sensibili, queste possano essere “ascoltate” da concorrenti e/o persone non gradite.

Le piattaforme gratuite sono le più pericolose: se si usano per gioco è un conto, ma per lavoro devono essere evitate.

LA COMUNICAZIONE VIA INTERNET



LA COMUNICAZIONE VIA INTERNET
Tecnologia «responsive»

Per verificare se il tuo sito web è ottimizzato per i dispositivi mobili
https://search.google.com/test/mobile-friendly


grazie
merci
arigatô
danke
gracias
thank you
shukran
tänan
dankie
obrigado
hvala
takk
tak
faleminderit
благодаря
kiitos
dank u
dhanyavād
terima kasih
paldies
diolch
köszönöm
mh'gōi
xièxiè
choukrane
grazzi
ďakujem
dziękuję
děkuji
mahalo
gràcies
tack
дякую
баярлалаа
хвала
спасибо
ngiyabonga
kop khun
multumesc
ačiū
teşekkür ederim
nandri
a dank
благодарам