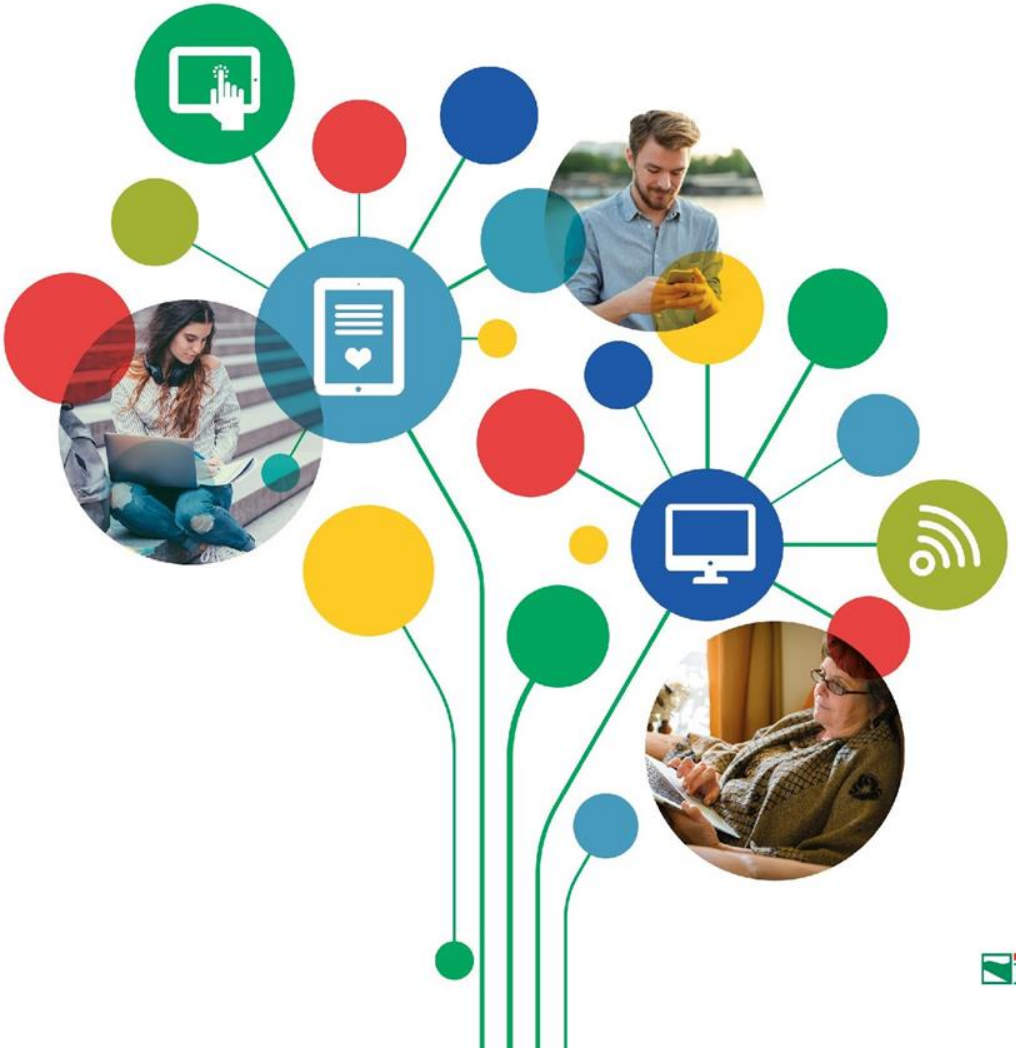


Pane e internet

Cittadini 100% digitali

Sei sicuro? Consigli pratici di sicurezza digitale

#Nome-Cognome Relatore

RegioneEmiliaRomagna

AgendaDigitale ER

Emilia-Romagna facciamo la differenza.

per la cultura e i saperi

Il progetto Pane & Internet

È un progetto finanziato dalla Regione Emilia-Romagna, nell'ambito dell'Agenda Digitale Regionale
Ha l'obiettivo di favorire lo sviluppo delle competenze digitali dei cittadini al fine di garantire una piena cittadinanza digitale.
Il "cittadino digitale" è un cittadino che, a tutte le età, usa le tecnologie per accedere alle informazioni, per fruire di servizi sempre più avanzati e per cogliere le opportunità che il digitale offre nel suo territorio.
Si snoda nel territorio attraverso la rete di Punti Pane e Internet e collabora costantemente con biblioteche, scuole e associazioni, ecc.

IMPARIAMO A DIFENDERCI

L’evento che tratteremo in questo incontro (durata 2h)

Durante l’incontro verranno discusse le principali tematiche relative al mondo della sicurezza informatica, cercando di rispondere a domande spesso molto comuni, ovvero:

- Come possiamo proteggere i nostri dispositivi?
- Cosa sono i messaggi crittografati?
- Cosa si intende per antivirus e protocollo di sicurezza, ecc.?

Quali punti toccheremo?

L’indice dei principali argomenti trattati da questa presentazione:

- Cosa si intende per sicurezza informatica?
- I principali attacchi che possiamo subire
- Chiudiamo le porte a possibili attacchi (comportamento umano, scelta antivirus, autenticazione 2FA)
- Proteggersi su device mobile e IOT
- Brevi cenni sulla crittografia
- Protocolli di sicurezza nella navigazione web

Cosa si intende per sicurezza informatica

Una breve definizione

La cybersecurity è la pratica che consiste nel **difendere i computer e i server, i dispositivi mobili, i sistemi elettronici, network e dati da attacchi pericolosi**. È anche conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche.

Il termine abbraccia un ampio raggio di settori e **si applica a qualunque cosa**: dalla sicurezza dei computer al ripristino di emergenza e all'istruzione degli utenti finali.

Kaspersky Lab 2019

Valutazione del rischio informatico

Le diverse tipologie di attacco

Quali sono i principali attacchi informatici che possiamo ricevere?

- **Malware e trojan e virus** (Cybercrime)
- Attacchi **Man in the middle** (Cyberspionaggio, non tratteremo questa tipologia)
- **Phishing** (Cyberspionaggio, tentativi di truffa)
- **Spam** (via mail, sms o telefonico)

Valutazione del rischio informatico

Gli attacchi informatici nel 2018

Dati del rapporto Clusit relativi al I semestre

Cybercrime · Cyberspionaggio · Attacchi "Multiple Targets" (verso più obiettivi)
malware semplice · ransomware

730 attacchi gravi registrati

+31% sul 2017

+35% **+69%** **+15%**

I vettori più utilizzati

+22% **+21%**

I settori più colpiti

automobilistico	+200%
ricerca-educazione	+128%
ospitalità	+69%
sanità	+62%
istituzioni	+52%
cloud	+52%
consulenza	+50%

61% delle tecniche utilizzate
phishing e malware

ANSA centimetri

Qualche dato (fonte Ansa 2018)

- I principali attacchi derivano da **Phishing e Malware**
- C'è stato un **aumento** del 31% rispetto all'anno precedente
- Il Cyberspionaggio rappresenta nel nostro paese una delle cause maggiore di attacchi informatici

I principali attacchi informatici

Malware, trojan e virus

La triade composta da: malware, trojan e virus costituisce un insieme di elementi utili all'hacker per raggiungere un vasto numero di utenti al fine di trafugare informazioni, chiedere eventuali riscatti o semplicemente arrecare disservizio.

Malware: (abbreviazione di malicious software), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer, replicandosi.

Trojan: nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo. L'utente, eseguendo quest'ultimo programma, attiva anche il codice del trojan nascosto.

Virus: programma o applicativo che ha come unico obiettivo quello di distruggere un sistema informatico, a volte può replicare e diffondersi via mail, sono i predecessori dei malware.

I principali attacchi informatici - Phishing

Il PHISHING ed il mail spoofing

Questa tipologia di attacco ha lo scopo di creare delle vere e proprie trappole
in grado di costringere l'utente che le subisce a rilasciare informazioni personali sensibili come ad esempio:

- **Credenziali** di login (Username e Password) per accedere ad un determinato sito web
- Numeri di **carte di credito** (Numero, scadenza e CVV)
- **Informazioni personali** specifiche (Dati sensibili)

I principali attacchi informatici - Phishing

Come avviene un attacco di PHISHING

Un classico attacco di Phishing è quello che si riceve molto spesso via mail, caratterizzato da una “finta” mail ben costruita che a volte può mandare in confusione anche utenti più esperti.

L’attaccante SIMULA di essere un addetto di: banche, servizi postali, servizi intermediari di carte di credito, inviandoci una mail dove viene richiesto di effettuare l’accesso ad un sito che molto spesso “maschera” il proprio indirizzo.

Vediamo un esempio...

I principali attacchi informatici - Phishing

Un esempio di mail phishing

Nella mail a fianco notiamo alcuni elementi sospetti, come:

- Indirizzo mail mittente
- Il testo poco formale, che a volte può contenere errori ortografici
- Il link da cliccare per ottenere il fantomatico rimborso

Chiudiamo le porte ai possibili attacchi

Le buone pratiche da seguire

1. ***La scelta delle proprie credenziali di accesso***

Una buona pratica per incrementare il livello di sicurezza su servizi che richiedono username e password passa dai seguenti punti:

- Scelta di una **password complessa**, lunga almeno 10 caratteri, contenente lettere maiuscole/minuscole, almeno un numero ed un simbolo (&,%,-,/)

- **Utilizzare password differenti** per ogni servizio o per ogni classe di servizio (es. utilizzo una password per i servizi bancari, la modifico per la mail e ne uso un’altra per tutti i restanti servizi)

Chiudiamo le porte ai possibili attacchi

(continua) - La scelta delle proprie credenziali di accesso

- Autenticazione a 2 fattori: conosciuta con il termine **2FA** permette di avere un ulteriore strato di sicurezza. In prima fase viene richiesta la combinazione user e password, terminata questa fase per accedere al servizio verrà inviato un codice sullo smartphone o su un'app.

Chiudiamo le porte ai possibili attacchi

Le buone pratiche da seguire

2. Utilizzo di un buon antivirus

La buona pratica consigliata è valida sopratutto per avere un supporto maggiore in caso di attacchi subdoli, Windows dalle sue ultime versioni integra un Antivirus gratuitamente.

Alcuni link per aiutarci nella scelta:

- Altroconsumo: https://www.altroconsumo.it/hi-tech/smartphone/test/app-antivirus
- AV Comparison: https://www.av-comparatives.org/comparison/
- AV Test: https://www.av-test.org/en/

Chiudiamo le porte ai possibili attacchi

Le buone pratiche da seguire

3. Mantenere il proprio software aggiornato

Questo consiglio vale sia per PC che per dispositivi mobile e IoT, segui queste piccole regole:

- Prediligi software aggiornato in fase di acquisto di un nuovo dispositivo
- Effettua gli aggiornamenti automatici
- Non installare software da fonti sconosciute
- Non scaricare software pirata (sembra banale ma è uno dei primi vettori di malware e key logger)

Chiudiamo le porte ai possibili attacchi

Le buone pratiche da seguire

4. La prima tua difesa è la conoscenza

Questo consiglio è strettamente collegato alla necessità di stimolare la propria cultura digitale:

- Evitare di aprire mail con richieste di login, in caso di familiarità con i contenuti della mail verificare sempre il mittente.
- Scarica file solo da siti certificati, apri gli allegati mail solo da persone che realmente conosci
- Non installare software da fonti sconosciute

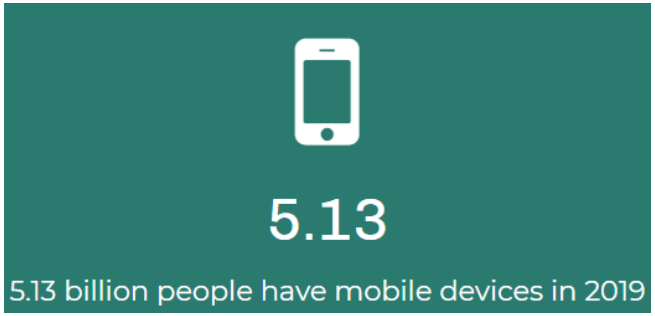
Proteggersi su device mobile e IoT

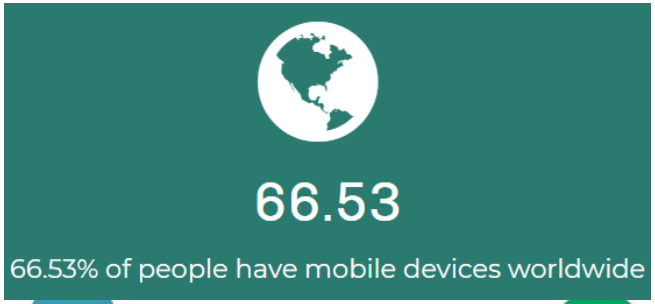
'.o smartphone come canale di accesso

Il nostro smartphone non è esente da compromissioni o attacchi informatici, essendo un dispositivo **perennemente connesso** alla rete e dotato di potenza di calcolo sempre crescente oltre che di dati sensibili.

Proteggersi su device mobile e IoT

Attacchi hacker su smartphone e tablet, qualche dato





Il bacino **potenziale** di smartphone attaccabili è pari al 66% delle persone che popolano il pianeta.
Quali sono le minacce più diffuse su smartphone e tablet?

- Invio di SMS non autorizzati
- Malware
- Phisihng (analogamente a quanto visto per PC)

Fonte dati: bankmycell.com 2019

Proteggersi su device mobile e IoT

Le tipologie di attacco su smartphone

Invio di SMS non autorizzati e abbonamento a servizi

Questa tecnica non viene propriamente definita un “hack” ma sfrutta l’inganno oltre alla scarsa conoscenza del navigare sicuri all’interno del web.

Il problema: l’utente navigando su smartphone e tablet all’interno di siti web, cliccando accidentalmente banner o elementi “attraenti” attiva sulla propria SIM card abbonamenti a seriviz di SMS a pagamento.

La soluzione: se si notano continui addebiti sul proprio credito o è necessario effettuare spesso ricariche telefoniche, potrebbe essere utile **rivolgersi immediatamente al servizio clienti del proprio operatore telefonico** per bloccare i servizi in abbonamento.

Proteggersi su device mobile e IoT

Le tipologie di attacco su smartphone: i Malware

Malware e app non sicure

Questo attacco sfrutta veri e propri “cavalli di Troia” per creare porte aperte disponibili per accedere a tutti i dati presenti sul dispositivo della vittima.

Il problema: l’utente non ha più il controllo del proprio telefono e subisce la perdita dei propri dati, il furto della propria identità o dati bancari.
Questi problemi si presentano a seguito dell’installazione di nuove app sul proprio dispositivo, talvolta l’hacker può attuare manovre di “sequestro” dei dati chiedendo poi un riscatto (Ransomware).

Proteggersi su device mobile e IoT

Le tipologie di attacco su smartphone: i Malware

La soluzione: per ridurre al minimo il rischio di questi attacchi, possiamo seguire alcune accortezze.

1) Non scaricare app da origini sconosciute, utilizza soltanto app presenti sugli store del proprio telefono; Google Play per **Android** e App Store per **iOS** (iPhone e iPad).

2) Utilizzare reti wifi sicure, evitando il più possibile di utilizzare reti wifi libere e gratuite che potrebbero essere **controllate e filtrate**.

3) Effettuare gli **aggiornamenti previsti** al sistema operativo e alle app installate (non rimandare!)

Proteggersi su device mobile e IoT

Come dobbiamo comportarci con i dispositivi iOT

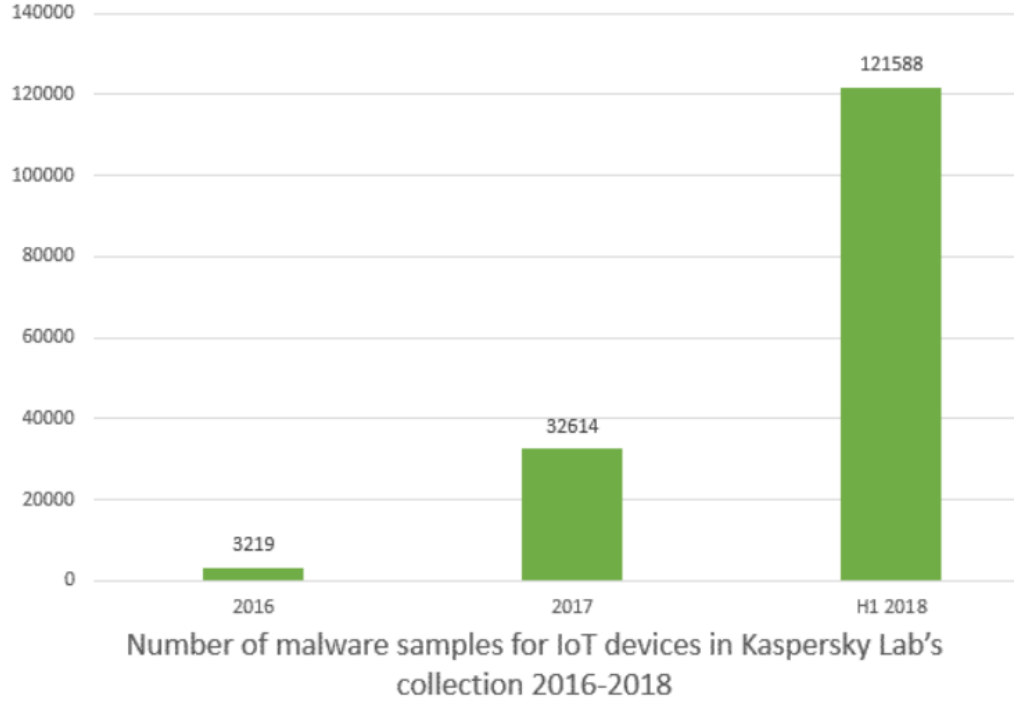
Il crescente uso di dispositivi di iOT
(IoT o idC, acronimo italiano di Internet delle cose)
come:

- Telecamere di sicurezza (Interne ed Esterne)
- Sistemi di domotica (Controller, centraline, interruttori)
- Elettrodomestici intelligenti (Smart TV, Frigo smart, ecc…)

ha determinato un **ulteriore canale per la diffusione di attacchi informatici**. Non solo, questi dispositivi i casi molto selezionati e al momento rari, offrono punti di attacco a coloro che intendono spiare la nostra vita privata.

Proteggersi su device mobile e IoT

Qualche dato



Number of malware samples for IoT devices in Kaspersky Lab's collection 2016-2018

Nel 2018 sono stati stimati 121k attacchi su devices iOT, ma qual'è lo scopo di questi attacchi?

- Creazione di **BOTNET**, ovvero hackerare il dispositivo per utilizzarlo come elemento con il quale attaccare altri target.

- Violazione della privacy personale

Fonte: Kaspersky Lab's 2016-2018

Proteggersi su device mobile e IoT

Come difendersi da attacchi su dispositivi IOT

Per difendere al meglio i nostri dispositivi e devices IOT possiamo seguire alcune semplici regole:

1. **Aggiornare** il firmware e/o il sistema operativo del nostro devices
2. **Modificare le password** di accesso che vengono inserite di default dal costruttore (Es. videocamere di sorveglianza o router adsl/fibra)
3. Acquistare **dispositivi affidabili**, certificati per il nostro mercato e di marchi conosciuti

Con queste 3 semplici regole non avremo il 100% di sicurezza ma potremmo dire di aver fatto il possibile per ***rendere la nostra casa ed i nostri dispositivi più sicuri.***

Brevi cenni sulla crittografia

Cosa si intende per crittografia

L’etimologia aiuta a capire: Kryptós (nascosto) e graphía (scrittura) sono le due parole greche che compongono il termine crittografia. Consiste in un sistema pensato per rendere illeggibile un messaggio a chi non possiede la soluzione per decodificarlo.

Perché si usa:

- **Ridurre attacchi** man in the middle
- **Proteggere** le comunicazioni tra due persone
- **Tutelare** la propria privacy

Brevi cenni sulla crittografia

Software e app di consumo

Ecco un breve elenco di software e applicativi che utilizzano sistemi di crittografia per l'invio e la ricezione di messaggi tra due persone:

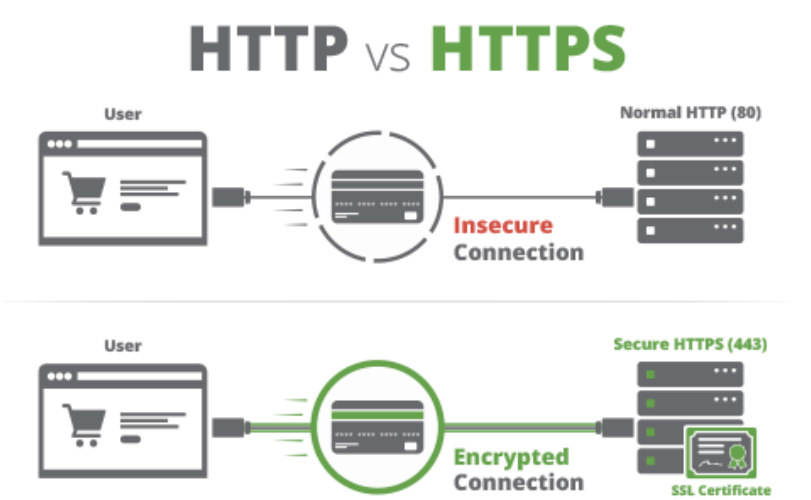
- **Wathsapp e Telegram**, l'invio di messaggi è criptato nella modalità chat privata
- **Proton Mail**, utile per inviare mail criptate
- **Truecrypt**, utile per creare un'area sicura contenente file o dati

Attenzione, nel caso utilizziate sistemi di crittografia per i vostri file o porzioni di hard disk, è bene conservare la propria chiave privata in un luogo sicuro, è il vostro unico modo di accedere al contenuto dei file e del messaggio originale.

Sicurezza per la navigazione web

Protocolli e funzionamento

Quando digitiamo un indirizzo sul browser, richiediamo quasi sempre ad un server web contenuti da mostrare, il passaggio viene definito con il termine “connessione”



La connessione ad un sito web può essere di due tipologie:

- **Insicura** (http://) utilizzata in siti dove non c’è scambio di informazioni sensibili, ad es. siti di lettura e consultazione
- **Sicura** (https://) utilizzata per siti e-commerce, banche, sistemi di pagamento o siti dove è richiesta la registrazione dell’utente.

Sicurezza per la navigazione web

HTTPS e protocollo SSL

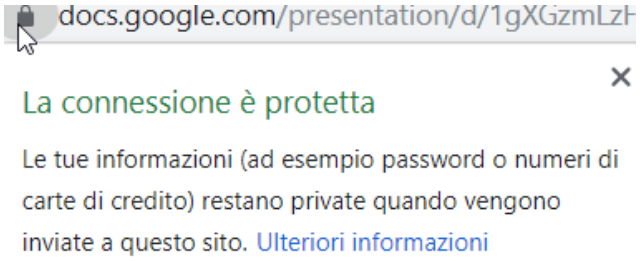
Perché ha senso utilizzare una connessione sicura?

Il motivo riprende il concetto di crittografia, utilizzare una connessione sicura permette di tutelare il passaggio di informazioni sensibili (numeri di cc, credenziali e login…) tra il nostro PC ed il sito web.

Come faccio a capire se la mia connessione è sicura?

Se dobbiamo effettuare acquisti su siti e-commerce, pagamento di bollette, operazioni bancarie ecc… è importante che sulla barra degli indirizzi sia presente l'indicazione di protocollo SSL, o indicazioni più generiche di **connessione protetta**.

Ecco cosa dobbiamo verificare quando visitiamo un sito web:



paneeinternet.it