Pane e internet

Cittadini 100% digitali

SICUREZZA DIGITALE QUOTIDIANA PER TUTTI

Prima la persona, e poi le password

Stefano Castelli

Consulenze e servizi per il mondo digitale

RegioneEmiliaRomagna AgendaDigitale ER DATAVALLEY bene comune ER

Il progetto Pane e 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.

Sicurezza informatica

Cosa intendiamo con «sicurezza informatica»?

La cosiddetta «*cybersecurity*» è un insieme di pratiche estremamente sofisticate che hanno a che fare con la protezione di dati, siti, applicazioni e in generale di ogni tipo di informazione visibile tramite le reti informatiche.

Governi, aziende grandi e piccole, privati: ognuno di noi ha a che fare con questo, quotidianamente.

Sicurezza informatica

I governi?

Le elezioni americane con Trump vincitore e le ombre russe, governi come Russia, Cina, Iran, USA, Corea del Nord, Israele: sono solo alcuni esempi di dominio informatico e hacking continuo (la Merkel spiata dai Russi), ma anche degli alleati (lo spionaggio sistematico degli alleati Nato da parte del governo USA).

https://it.wikipedia.org/wiki/National_Security_Agency

https://it.wikipedia.org/wiki/ECHELON

Ma gli hacker sono cattivi?

I media tradizionali come la tv, per ignoranza e facile sensazionalismo, chiamano «hacker» i cattivi del web.

Ma è sbagliato. Ci sono hacker (tendenzialmente buoni e utili, detti «white hat» = cappello bianco), cracker (quelli cattivi, detti anche «black hat») e lamer (aspiranti cracker = imbranati).

https://tecnouser.net/differenza-hacker-cracker-lamer

Sicurezza informatica

Gli hacker sono buoni?

Non c’è uno spartiacque preciso. Spesso sono motivazioni economiche, ideologiche, ecc che spingono le persone - qualche esempio:

https://it.wikipedia.org/wiki/Anonymous (attivismo vario)

https://it.wikipedia.org/wiki/Julian_Assange (Wikileaks)

Sicurezza assoluta e relativa

La sicurezza totale semplicemente non esiste

Come in «*mission impossible*» con Tom Cruise:

non esistono sistemi informatici completamente sicuri.

Ogni sistema ha le sue falle: quelli fatti molto bene

Ne hanno pochissime e difficili da scovare,

Quelli fatti male ne hanno parecchie.

Vita digitale

Ma siamo on line oppure off line?

Una volta esisteva la differenza off line / on line…

MA oggi…

Vita digitale

Email, foto, social, gps, video… aiuto! ☺

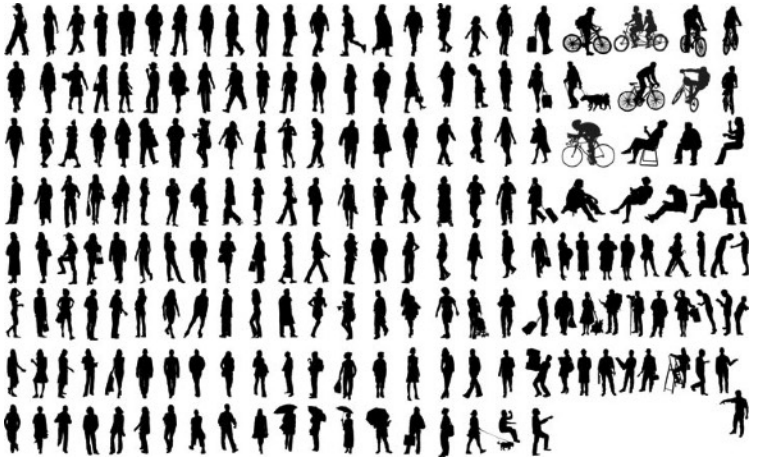
Già, pare proprio che oggi non siamo più davvero offline:

quasi mai…

Qualche esempio?

- GPS
- Video e foto
- Social network

OK, chiudo tutto e me ne vado…



Fuggire o lasciar perdere, arrendendosi?

La buona notizia è che il livello di cui abbiamo parlato è altissimo.

Richiede grandi capacità, risorse economiche, investimenti, ecc.

A noi cittadini comuni cosa capita in realtà?

Autodifesa digitale quotidiana

Le disavventure più comuni delle persone «normali»

- Furto di dati (carta di credito, e-banking, password varie… e faccio cose cattive)
- Furto di identità (prendo controllo dei tuoi social e faccio cose cattive)
- Hacking della posta (ci entro, cambio la password e faccio cose cattive)
- Truffe varie (cose cattive a prescindere: phishing, siti fraudolenti, finte raccolte fondi, ecc.)
- Virus o «malware» (trojan, worm, ransomware e compagnia ~~bella~~ brutta)
- ricatti sessuali via email

Autodifesa digitale quotidiana

Le nostre contromosse

- Password sicure e diversificate
- Autenticazione a due fattori – OTP
- Aggiornamento del computer
- Antivirus
- **Ma soprattutto… INTELLIGENZA, PRUDENZA, ATTENZIONE, MA SENZA PARANOIA**

Autodifesa digitale quotidiana

Password sicure

- Come crearle - https://www.recovery-data.it/come-creare-password-sicure-regole-da-seguire/
- Password più comuni: https://www.alyfa.net/le-25-password-piu-usate/
- Password diverse tra loro per i vari servizi
- ricordare le password (tecniche base): no https://www.ottimizzazione-pc.it/tecniche-per-creare-una-password-sicura-e-facile-da-ricordare/ e no http://www.iomemorizzo.it/ricordare-codici-password/
- password principale / passphrase (acronimi)
- conserva password: app/software | device fisici: chiavette, file nascosti

Autodifesa digitale quotidiana

Gestione password

- Aranzulla santo subito! Programmi vari: https://www.aranzulla.it/programmi-per-password-28420.html
- Chrome https://it.safetydetectives.com/best-password-managers/chrome/
- Firefox: https://addons.mozilla.org/it/firefox/search/?q=password%20manager

Crittografia? E cosa è???? Un esempio: HTTPS -> https://www.computernext.it/cose-il-protocollo-https/

Autodifesa digitale quotidiana

Gestione password

- Aranzulla santo subito! Di nuovo…
- LastPass @Aranzulla: https://www.aranzulla.it/gestore-di-password-lastpass-3952.html
- LastPass: come funziona https://www.lastpass.com/it/how-lastpass-works
- Lastpass: prezzi e opzioni https://www.lastpass.com/it/pricing
- Lastpass: video intro 2 min https://www.youtube.com/watch?v=IfVwrfDLHzA
- Lastpass: guida 24 min https://www.youtube.com/watch?v=XD9lyAyqi1A

Autodifesa digitale quotidiana

Autenticazione a due fattori & CO.

- Inserisco la password E POI…
- Uso un software apposta per codici segreti generati ogni 30 secondi (vedi authenticator e altre app)
- Attivo OTP (One Time Password), che arriva spesso sul telefono tramite SMS oppure via email.

Semplice, ma garantisce un'alta sicurezza

Ormai si può fare con quasi molti software, ad esempio gmail: https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=it

Autodifesa digitale quotidiana

Gli strumenti: computer, tablet, telefoni

- Aggiornamento del computer (aggiornamenti automatici ON, sempre!!!!)
- Aggiornamento del telefono (problema: spesso su Android dopo un paio di anni non vengono più rilasciati)
- Aggiornamento antivirus (come funziona un antivirus? Riconosce il codice dei virus, per cui se non è aggiornato, non li vede…)
- Backup dei dati (i ransomware non perdonano – vedi Wannacry nel 2017)

https://www.aranzulla.it/programma-per-fare-backup-dati-gratis-14033.html

https://www.aranzulla.it/antivirus-gratis-in-italiano-ecco-i-migliori-9244.html

https://it.wikipedia.org/wiki/WannaCry

Dicevamo…

… INTELLIGENZA, PRUDENZA, ATTENZIONE, MA SENZA PARANOIA

Un po’ di esempi reali e quotidiani:

- la sicurezza come atteggiamento: l'anello debole spesso è la persona, non il computer
- prudenza nelle mosse: se mi chiedono password ecc. cosa faccio?
- verifica dei dati: contatti, richieste, servizi realmente sottoscritti, chiamare persone e banche ecc.
- attenzione sì, ma senza paranoia! Chiudersi alle nuove possibilità non è la soluzione ☺
- ingegneria sociale: dai tuoi account social ottengo molte informazioni: nome cane, data nascita figli, ecc. – ecco, evitiamo queste informazioni nelle nostre password!

paneeinternet.it