TRUST aWARE

FONDAZIONE Mondo Digitale

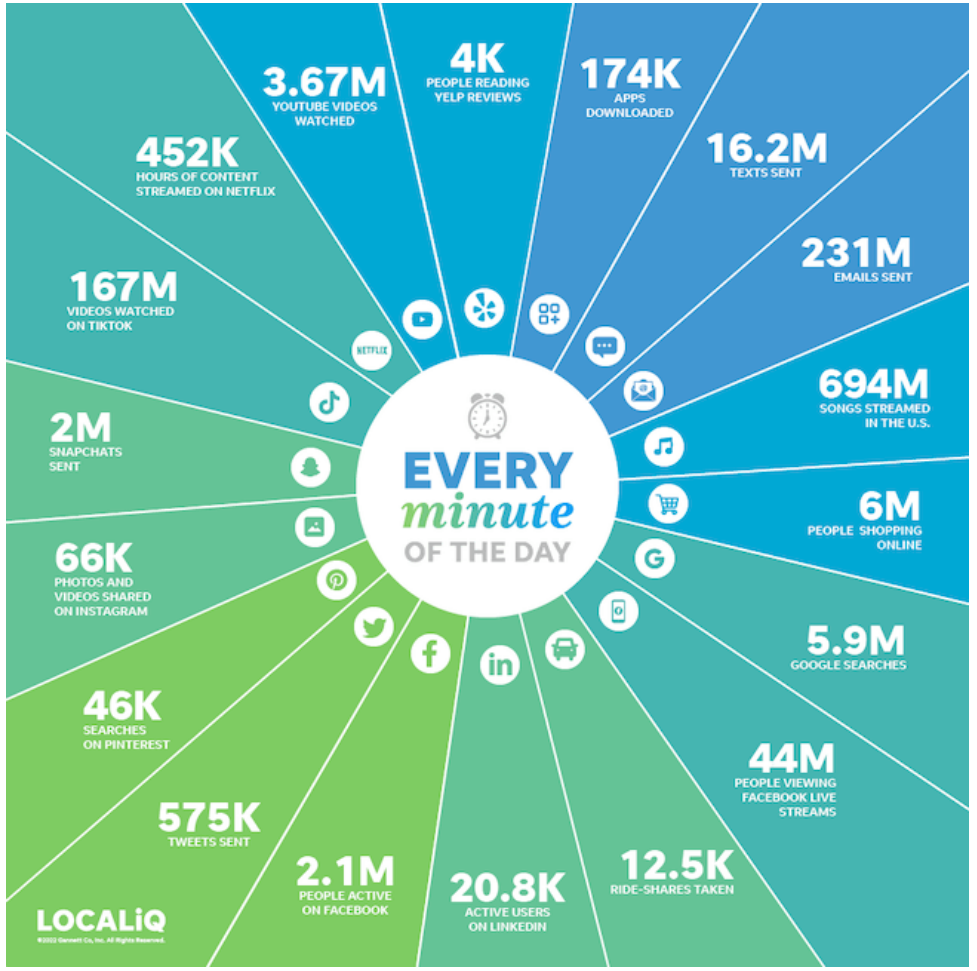
Enhancing Digital Security, Privacy and TRUST in softWARE

Antivirus & Password

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Index

Cosa succede in 1 Minuto online - 2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cybercrime & Cybersecurity

Condividiamo quotidianamente un numero enorme di dati utilizzando i nostri account digitali che sono, in qualche modo, tutti collegati tra loro.

La sicurezza deve essere il nostro primo obiettivo, nella vita online come in quella offline!

Gli stessi “crimini” che possono accadere nella vita quotidiana possiamo ritrovarli in rete: in questo caso si parla di **CYBERCRIME** da cui cerchiamo di difenderci grazie agli strumenti di **CYBERSECURITY**

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Cyber Crimine

Cybercrime: termine che indica una situazione di criminalità online che sfrutta in maniera estrema le funzioni hardware e software.

I Cyber attacchi possono avere 3 scopi principali:

- Cyber Crimine
- Cyber Attivismo
- Cyber Terrorismo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cyber Crimine

Cyber Crimine: Crimine finalizzato allo sfruttamento commerciale della rete internet, a porre a rischio i sistemi informativi di sicurezza nazionale attraverso attacchi informatici perpetrati in rete

Gli **attacchi informatici** sono tentativi indesiderati di sottrarre, esporre, alterare, disabilitare o eliminare definitivamente informazioni tramite l'accesso non autorizzato ai sistemi informatici.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cyber Crimine

Cyber Attivismo: Crimine finalizzato alla raccolta di dati non pubblici per scopi politici o macroscopici.

L'obiettivo è impossessarsi di informazioni che possono essere re-immesse in rete a favore/sfavore di un determinato contesto politico, sociale, economico, lavorativo, ecc

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cyber Crimine

Cyber Terrorismo: Crimine finalizzato al provocare panico e paura nella popolazione (digitale e non) per raggiungere momenti di tensione, caos e destabilizzare l'ordine interno finora mantenuto.

Si applica spesso a motivazioni politiche, economiche e sanitarie.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cybersecurity

Per combattere il CyberCrimine abbiamo bisogno di strumenti di difesa che vengono raggruppati sotto il nome di **CyberSecurity.**

Categorie di Cybersecurity:

- **Sicurezza delle Reti**
- **Sicurezza delle Applicazioni**
- **Sicurezza delle Informazioni**
- **Sicurezza Operativa**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cybersecurity

Sicurezza delle Reti: sistemi di sicurezza sviluppati per la protezione delle reti informatiche

Sicurezza delle Applicazioni: sistemi di sicurezza sviluppati per la protezione di tutti i dati e i contenuti che le app installate sui device tecnologici dovranno gestire; questo livello di sicurezza viene applicato prima che l'app sia disponibile per il download

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cybersecurity

Sicurezza delle Informazioni: sistema di sicurezza sviluppato per proteggere i dati archiviati ovunque online, sia in archivi permanenti che temporanei

Sicurezza Operativa: sistema di sicurezza sviluppato per la sicurezza dell'utente in rete; l'utente potrà scegliere di volta in volta come tutelare i propri dati personali e sensibili e le proprie azioni online gestendo i consensi.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cyber Attacchi: Il Malware

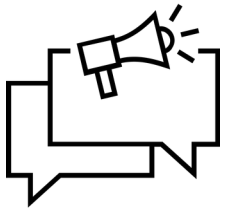
Malware: software che, una volta eseguito, danneggia il funzionamento e la sicurezza del sistema operativo; il termine deriva dalla contrazione di *malicious* e *software* e significa letteralmente “programma malvagio”.
Sempre più diffusi, i m. si trasmettono via internet; spesso tramite la posta elettronica, ma anche attraverso la semplice navigazione.*

*definizione Treccani

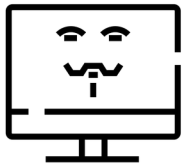
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Tipi di Malware

- **AdWare**: strumento che permette di far visualizzare all'utente pubblicità indesiderata



- **Ransomware:** strumento che congela il PC per una successiva richiesta di riscatto



- **SpyWare**: strumento che spia l'utente a sua insaputa

- **Rootkit**: strumento che permette l'accesso da remoto al pc dell'utente vittima

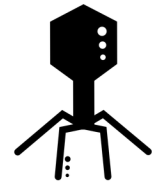
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Tipi di Malware

- **Worm**: programma in grado di replicarsi autonomamente sfruttando le reti e le falle di sistema per il furto di dati o la cancellazione di file

- **Trojan Horse:** strumento spesso nascosto dagli hacker in file allegato a e-mail di phishing (esempio, file Word) che, una volta scaricati e aperti, installano sul pc un malware

- **Virus**: esattamente come quelli reali, può copiarsi, unirsi ad altri programmi e diffondersi in altri computer



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Il Malware: come individuarlo

Quali sono i “segni” che ci fanno capire che ci troviamo di fronte a un device infettato da malware:

- Diminuzione delle prestazioni e della velocità del device;
- Apertura incontrollata di finestre pop-up che invadono lo schermo e diventano difficili da gestire e chiudere in sicurezza;
- Blocco continuo del sistema e comparsa della schermata blu d’errore che ci notifica l’impossibilità del pc di funzionare correttamente;
- Aumenta inspiegabilmente dell’attività di rete del sistema;
- Modifica non autorizzata della home page del browser;
- Installazioni non autorizzate e improvvise di toolbar ed estensioni sconosciute nel browser;
- Malfunzionamento improvviso dell’antivirus

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Il Malware: come combatterlo

Consigli utili per proteggere i nostri device dai malware e da conseguenti malfunzionamenti o azioni di phishing:

- Installare sul PC un antivirus affidabile;
- Effettuare gli aggiornamenti di sistema dei device e quelli degli antivirus con regolarità e seguendo le indicazioni degli sviluppatori;
- Evitare di cliccare su link potenzialmente pericolosi e sconosciuti
- Non condividere nessun tipo di informazione sensibile con siti o utenti sconosciuti o poco raccomandabili;
- Non scaricare e aprire file (.doc, PDF, ecc) da e-mail inviate da indirizzi sconosciuti o segnalati come SPAM
- Non cliccare su pop-up ingannevoli
- Non pagare riscatti per lo sblocco del computer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

L'Antivirus

ANTIVIRUS

Software impiegato per prevenire, rilevare ed eliminare virus informatici, worm, trojan, dialer, spyware e malware.
Poiché un virus è composto da una determinata stringa di codice, il programma agisce cercando tale sequenza all'interno della RAM (*Random access memory*), nei file memorizzati e in quelli ricevuti mediante periferiche o posta elettronica.

*definizione Treccani

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

L'Antivirus

Il funzionamento di questo metodo si basa sull'aggiornamento costante degli schemi che il software è in grado di riconoscere. Un'impostazione alternativa, detta *euristica*, consiste nell'analizzare i programmi in esecuzione per riscontrare le istruzioni sospette in quanto caratteristiche del comportamento dei virus. Generalmente in un software a. un modulo principale esamina il disco rigido (scansione) ed elimina i virus eventualmente presenti, mentre un altro risiede in memoria (restando così sempre attivo) e rileva i virus nei file che vengono aperti.

*definizione Treccani

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Software anti-virus

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Software anti-virus

Bitdefender

adaware
keep on connecting

SCANGUARD
safe search

Malwarebytes

TOTAL AV
The Ultimate Antivirus

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password: sceglierne una efficace

La **Password** ci consente di limitare l'accesso ad un account privato e proteggere i nostri dati e contenuti.

La Password non deve:

- Essere condivisa con nessuno
- Essere la stessa per tutti gli account/device
- Essere troppo facile da indovinare
- Contenere date di nascita, nomi di persone care, squadre tifate, ecc
- Scritta in posti facili da scoprire (ad esempio, un foglietto nel portafoglio, su una lavagnetta in casa, in una rubrica in un cassetto di libero accesso, ecc..)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password: sceglierne una efficace

Per evitare di perdere le password o doverle cambiare ripetutamente, possiamo utilizzare un'app specifica: il gestore di password!

Ne esistono molte tipologie scaricabili sia per Android che per IoS, tra le più famose, sicure ed utilizzate:

- NordPass (a pagamento)
- Bitwarden (gratuita)
- Google Smart Lock

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password: sceglierne una efficace

Consigli per una password efficace:

- La **lunghezza**: minimo 8 caratteri
- La **complessità**: parole di scarso utilizzo o complessa scrittura
- La **grafia**: utilizzare lettere maiuscole e minuscole, numeri e caratteri speciali in maniera mista; sostituire le lettere con i numeri e viceversa (cane = c4n3 / 1980 = l98o)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password efficace: facciamo un check!

https://howsecureismypassword.net/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autenticazione a 2 Fattori: questione di sicurezza

L'**Autenticazione a 2 Fattori** (o verifica a due passaggi) è un livello di sicurezza maggiore che possiamo attivare sui nostri account Social.

Ci permette di bloccare qualsiasi tentativo di accesso da parte di un hacker.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autenticazione a 2 Fattori: questione di sicurezza

Attivandola, ogni qual volta si effettua l'accesso al nostro account da un browser/device sconosciuto, ci arriverà una notifica con orario, data e luogo dell'accesso.
In caso non fossimo noi, sarà possibile bloccare l'accesso e procedere con un cambio password.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autenticazione a 2 Fattori: questione di sicurezza

Come si attiva:

- Nelle impostazioni di Privacy e Sicurezza del nostro account Social
- Scegliere di attivare l'Autenticazione a 2 Fattori
- Scegliere la modalità:
  - Codice SMS
  - Codici di Sicurezza (lista di codici da utilizzare una sola volta e rigenerare al bisogno)
  - App di autenticazione (esempio: Google Authenticator)
- Completare la procedura guidata

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

Enhancing Digital Security, Privacy and TRUST in softWARE

Grazie per l’attenzione.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377