CYBER SECURITY AWARENESS
LA CULTURA DELLA SICUREZZA INFORMATICA

Brescia, 7 Marzo 2023

Argomento

- LE BEST PRACTICES CHE POSSONO PRESERVARCI

BEST PRACTICES

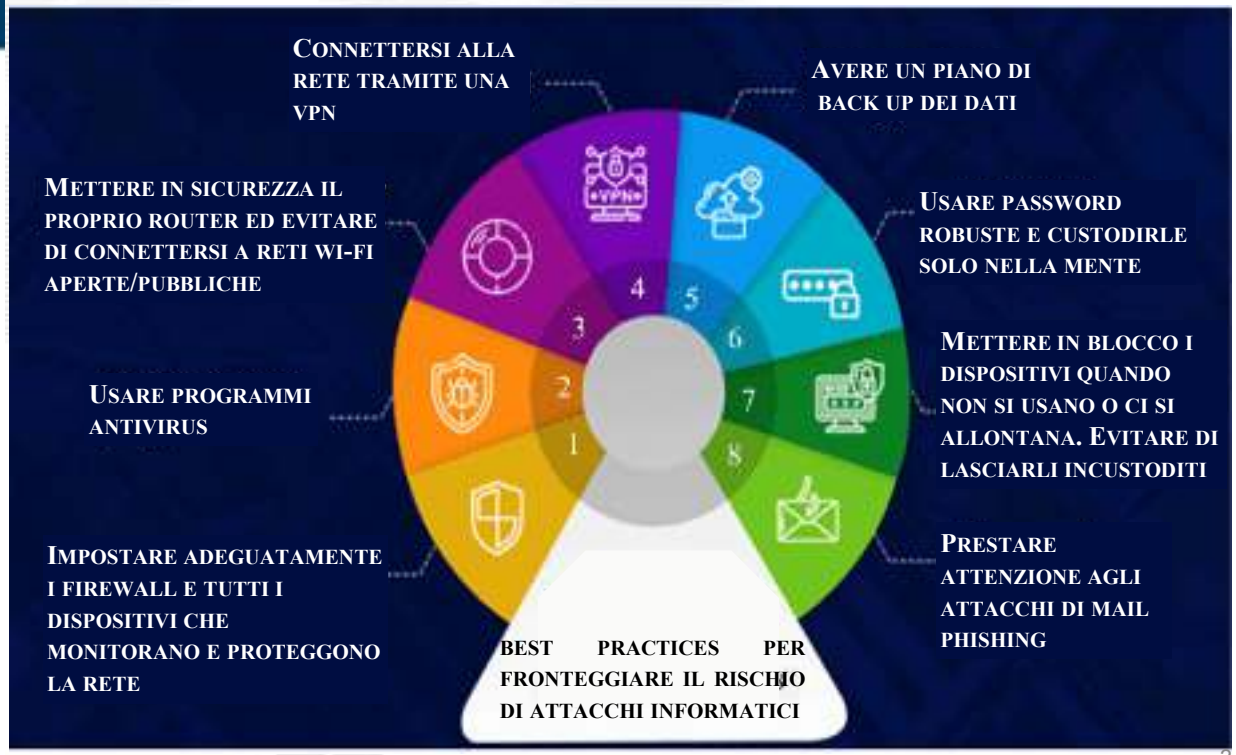
LE BEST PRACTICES CHE POSSONO PRESERVARCI

LE BEST PRACTICES SONO QUELLE AZIONI, COMPORTAMENTI, PIANI DI AZIONE E REAZIONE CHE, SE ADOTTATE, PERMETTONO DI MITIGARE IL RISCHIO DEL VERIFICARSI DI ATTACCHI INFORMATICI

Cyber Best Practices

SE NON STRETTAMENTE NECESSARIO, LIMITARE L'ESPOSIZIONE DEI DISPOSITIVI ALLA RETE INTERNET	USARE IL PIÙ POSSIBILE COMUNICAZIONI CIFRATE
UTILIZZARE UNA STRATEGIA DI PROTEZIONE DELLA RETE IN PROFONDITÀ	SEGUIRE BEST PRACTICES DOCUMENTATE PER METTERE IN SICUREZZA I SISTEMI E I DISPOSITIVI
NON LASCIARE LE CREDENZIALI DI FABBRICA DEI DISPOSITIVI, QUELLI DI RETE SOPRATTUTTO (ROUTER, FIREWALL, PROXY FILTER, …)	NON DIMENTICARE LA SICUREZZA FISICA (O DEL MONDO REALE)
TENERE AGGIORNATI I SISTEMI CON PATCH E UPGRADE	SOTTOPORRE UNA VALUTAZIONE FORMALE DELLA MINACCIA E DEL RISCHIO
PROTEGGERSI DAGLI ATTACCHI RANSOMWARE, EFFETTUARE UN BACK UP PERIODICO DEI DATI	NON DIMENTICARE LE PERSONE, I PROCESSI E LE TECNOLOGIE

https://www.realcomm.com/news/912/2/towards-a-cybersecurity-partnership-in-connected-buildings



https://www.researchgate.net/figure/The-best-practices-to-overcome-cyber-security-risks_fig3_348629997

BEST PRACTICES

RIGUARDO LE PASSWORD …

USARE PASSWORD LUNGHE CON CARATTERI ALFANUMERICI NUMERI E SIMBOLI SPECIALI E CHE SIANO FACILI DA RICORDARE.

EVITARE PASSWORD TROPPO SEMPLICI O MOLTO BREVI.

GLI HACKERS SANNO BENE CHE PUÒ ESSERE MOLTO COMPLICATO GESTIRE DIVERSE PASSWORD. SE RIESCONO AD IMPOSSESSARSI DI UNA PASSWORD, LA USERANNO CERTAMENTE PER L'ACCESSO AD ALTRI SERVIZI.

NON TRASCRIVERE O APPUNTARE LA PASSWORD PER NESSUN MOTIVO

BEST PRACTICES

RIGUARDO LE PASSWORD …

NON USARE LA STESSA PASSWORD PER ACCOUNT PERSONALI E PER IL LAVORO (USARE COMUNQUE PASSWORD DIVERSE PER I DIVERSI ACCOUNT CHE SI POSSEGGONO A PRESCINDERE CHE SIANO PERSONALI O PER IL LAVORO). USARE UN PASSWORD MANAGER PER FACILITARNE LA GESTIONE.

- UTILIZZARE ACCOUNT SEPARATI PER LAVORO E PER USO PERSONALE;
- UTILE UNA POLITICA DI SCADENZA DELLE PASSWORD.

FONTE: https://news.sophos.com/it-it/2019/03/04/i-password-manager-perdono-dati-in-memoria-bisogna-comunque-continuare-a-usarli/

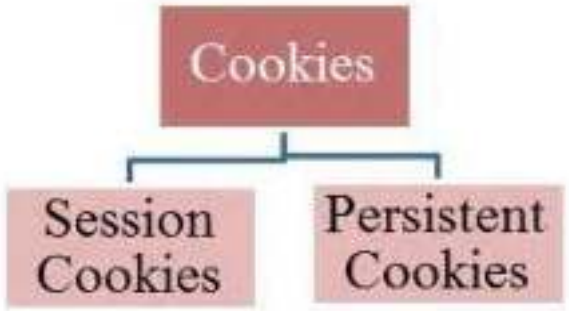
BEST PRACTICES

NON SALVARE MAI LE CREDENZIALI E LE PASSWORD NEI PROGRAMMI, APPS O BROWSER E PULIRE SPESSO LA CACHE DEI SOFTWARE CHE SI UTILIZZANO COME I BROWSER, ECC...

CREDEZIALI SALVATE NELLA CACHE DEL BROWSER E SUGGERITE

FONTE: https://www.spaceclick.com/it/blog/come-visualizzare-in-chiaro-le-password-immesse-dai-browser-o-nascoste-da-asterischi/

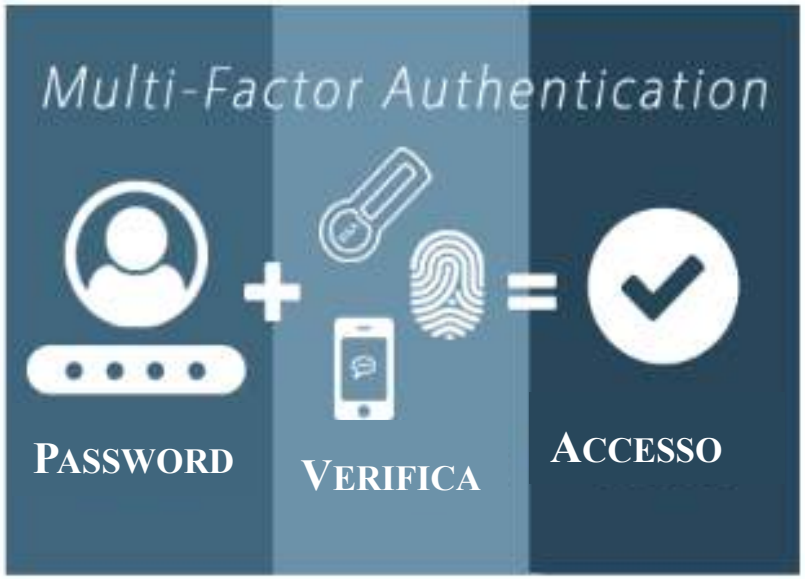
ID + password



Cookies

BEST PRACTICES

QUANDO DISPONIBILE, USARE LA MULTI-FACTOR AUTHENTICATION (AUTENTICAZIONE A DUE, TRE O PIÙ FATTORI)



PASSWORD USA E GETTA, CODICE RICEVUTO DA SMS

LA MULTI FACTOR AUTHENTICATION SI COMPONE DI DIVERSI ELEMENTI:

- QUALCOSA CHE SI CONOSCE (PASSWORD, CODICE);
- QUALCOSA CHE SI POSSIEDE (TOKEN, APP, SMARTPHONE);
- QUALCOSA DI COME SI È FATTI (IMPRONTA DIGITALE, RICONOSCIMENTO DEL VOLTO, DELL'IRIDE, ECC…);

ATTENZIONE PERÒ AI DATI BIOMETRICI (QUALCOSA DI COME SI È FATTI) PERCHÉ NON SI POSSONO CAMBIARE (NON È POSSIBILE CAMBIARE UNA CARATTERISTICA DI COME SIAMO FATTI).
SE UN MALINTENZIONATO RIUSCISSE A SOTTRARRE QUESTI DATI BISOGNEREBBE A QUESTO PUNTO RINUNCIARE AD USARLI COME DATI DI CONTROLLO/VERIFICA PER ACCEDERE AI NOSTRI SERVIZI (SERVIZI BANCARI, E-COMMERCE, IN GENERALE SERVIZI CHE GESTISCONO IL DENARO O DATI NOSTRI SENSIBILI)

BEST PRACTICES

GESTIONE DELLA PASSWORD

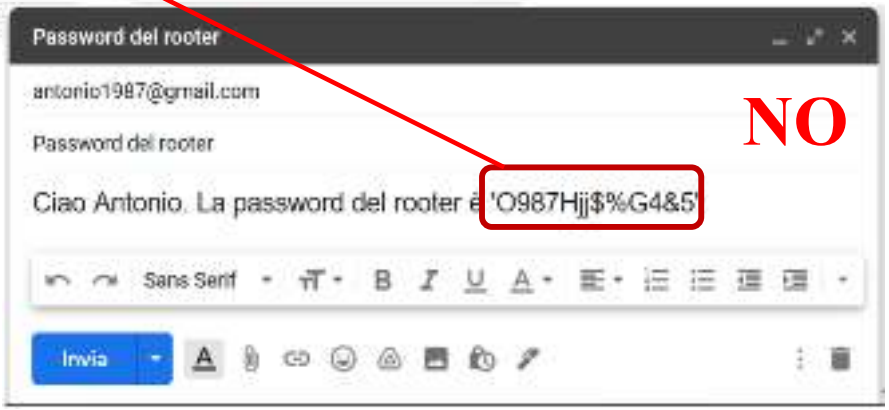
- EVITARE DI ANNOTARE LE PASSWORD O DI CONSERVARLE IN UN FILE DI TESTO O UN DOCUMENTO NON SICURO.

NO

FONTE: https://www.avg.com/it/signal/why-you-need-a-password-manager

PASSWORD NEL TESTO DELLA MAIL

- LA POSTA ELETTRONICA NON È UN SISTEMA DI GESTIONE DELLE PASSWORD. NON INVIARE MAI LA TUA PASSWORD A NESSUNO (INCLUSO TE STESSO). UN GESTORE DELLE PASSWORD È UN'OPZIONE UTILE PER LA MEMORIZZAZIONE DELLE STESSE. NE ESISTONO MOLTI CHE FUNZIONANO SU DESKTOP E DISPOSITIVI MOBILI. QUESTI CIFRANO LE TUE PASSWORD E MOLTI TI AIUTANO ANCHE A GENERARE PASSWORD COMPLESSE.



NO

- 1PASSWORD E LASTPASS SONO ESEMPI DI TOOL UTILI ALLA GESTIONE DELLE PASSWORD.

FONTE: https://www.ictsecuritymagazine.com/articoli/gestione-delle-credenziali-una-comparazione-tra-i-principali-strumenti-di-password-management/

BEST PRACTICES

SICUREZZA DELLE E-MAIL

L'ATTACCO ATTRAVERSO LA POSTA ELETTRONICA È TRA I PIÙ COMUNI E DI MAGGIOR SUCCESSO. PIÙ DEL 90% DEGLI ATTACCHI RIUSCITI PROVENGONO DA E-MAIL DANNOSE.

LE E-MAIL POSSONO CONTENERE DIRETTAMENTE ALLEGATI INFETTATI DA VIRUS E MALWARE OPPURE LINK A SITI WEB DANNOSI. TALVOLTA IL TESTO INDUCE LA VITTIMA A FORNIRE INFORMAZIONI PERSONALI, COME AD ESEMPIO NOME UTENTE E SOPRATTUTTO LA PASSWORD.

I CRIMINALI INFORMATICI STANNO DIVENTANDO SEMPRE PIÙ EFFICACI NELL'ELUDERE IL RILEVAMENTO: LA SOLA TECNOLOGIA NON BASTA PER BLOCCARE QUESTE MINACCE

GDPR BLACKMAIL ATTACK: I CYBER CRIMINALI SFRUTTANO LA CONOSCENZA DEL FATTO CHE ALCUNE ORGANIZZAZIONI NON SI SONO ANCORA ADEGUATE AI DETTAMI DEL REGOLAMENTO SULLA PRIVACY E CERCANO DI ESTORCERE DENARO MINACCIANDOLE, TRAMITE MAIL, DI RIFERIRE TUTTO A CHI DI DOVERE

BEST PRACTICES

E-MAIL: COSA FARE E COSA NON FARE…

COSA FARE…

- VERIFICARE SEMPRE IL MITTENTE DI UN MESSAGGIO
- PASSARE CON IL MOUSE SUI COLLEGAMENTI A PAGINE WEB (LINK) PRESENTI NEL CORPO DEL MESSAGGIO PER VERIFICARE DOVE PUNTANO (FARE ATTENZIONE AI SERVIZI DI ABBREVIAZIONE DELLE URL ES. BIT.LY CHE POTREBBERO OSCURARE LA DESTINAZIONE FINALE DEL SITO WEB)
- ESSERE SEMPRE SCETTICO NEI CONFRONTI DEI MESSAGGI CON ERRORI DI ORTOGRAFIA/GRAMMATICA, CHE CONTENGONO LOGHI IMPROPRI O CHE TI RICHIEDONO DI AGGIORNARE O VERIFICARE IL TUO ACCOUNT
- SEGNALARE SEMPRE LE E-MAIL SOSPETTE

COSA NON FARE…

- APRIRE UN ALLEGATO DA UN MITTENTE SCONOSCIUTO
- FARE CLIC SU UN COLLEGAMENTO DA UN MITTENTE SCONOSCIUTO;
- INVIARE A TERZI IL TUO NOME UTENTE O LA TUA PASSWORD.

FONTE: https://www.cyberguru.it/2020/05/25/cyber-card-11-lo-smartworking-al-tempo-del-covid-19-copyle-3-tipologie-piu-comuni-di-attacco-phishing/

BEST PRACTICES

NAVIGAZIONE SICURA E CONTROLLI-AUTORIZZAZIONI DELLE APP

- MANTENERE AGGIORNATA LA VERSIONE DEL SOFTWARE DEL BROWSER.
- MANTENERE AGGIORNATI I PLUG-IN DEL BROWSER; IN PARTICOLARE ADOBE FLASH E JAVA, POICHÉ SONO SPESSO PRESI DI MIRA.
- VERIFICARE GLI INDIRIZZI E I COLLEGAMENTI (IN GENERALE GLI URL) PASSANDOCI CON IL MOUSE SOPRA PRIMA DI FARE CLICK.
- UTILIZZARE STRUMENTI PER IMPEDIRE DI APRIRE PUBBLICITÀ O POP-UP INGANNEVOLI E INDESIDERATI (USARE DEGLI AD BLOCKER).
- FARE ATTENZIONE QUANDO SI SCARICA SOFTWARE DA INTERNET.
- SE UN SITO WEB RICHIEDE INFORMAZIONI SULL'UTENTE DI QUALSIASI TIPO, ASSICURARSI CHE IL SITO WEB UTILIZZI IL PROTOCOLLO HTTPS. VERIFICARE IL LUCCHETTO O ALTRI INDICATORI (AD ESEMPIO INDIRIZZO CHE INIZIA CON 'HTTPS://').

FONTE: https://foerster-kreuz.com/internet-browser-persoenlichkeit/

UNA TORCIA NON DOVREBBE AVERE ALCUN MOTIVO PER RICHIEDERE L'ACCESSO AL NOSTRO ELENCO DI CONTATTI, POSIZIONE GPS, CRONOLOGIA DELLE CHIAMATE, GALLERIA DELLE IMMAGINI, …. ATTENZIONI AI PERMESSI CHE SI CONCEDONO ALLE APP

BEST PRACTICES

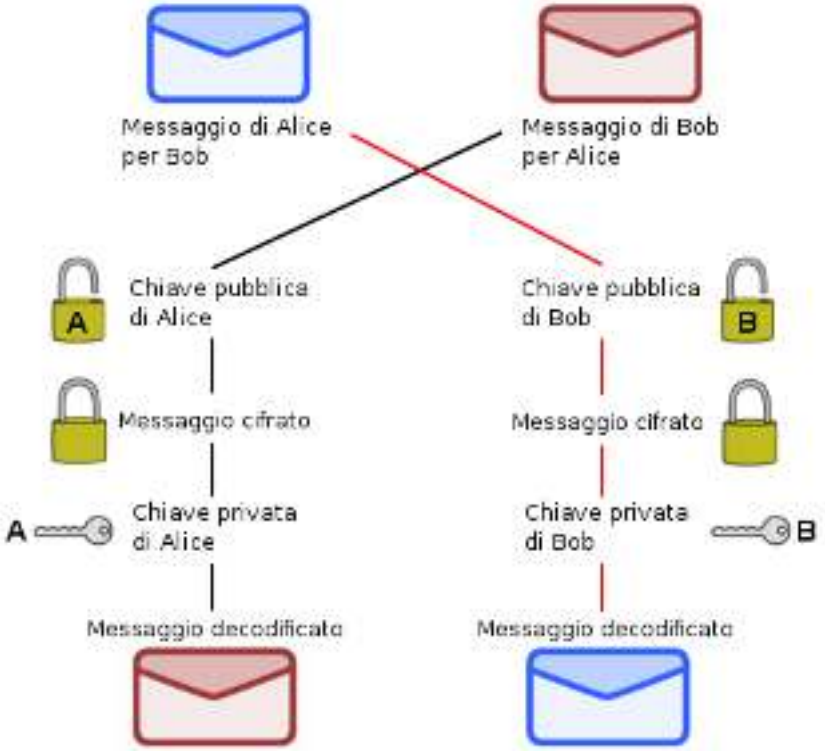
SICUREZZA DEI DISPOSITIVI MOBILI

- MANTENERE AGGIORNATO IL SOFTWARE DEI DISPOSITIVI: IL SOFTWARE SENZA PATCH RENDE I DISPOSITIVI VULNERABILE AGLI ATTACCHI.
- INSTALLARE GLI AGGIORNAMENTI DEL SISTEMA OPERATIVO E GLI AGGIORNAMENTI DELLE APPLICAZIONI.
- AVERE UN SOFTWARE ANTIVIRUS E/O ANTIMALWARE INSTALLATO, ABILITATO E IMPOSTATO PER L'AGGIORNAMENTO AUTOMATICO.
- NON LASCIARE MAI IL LAPTOP O DISPOSITIVO MOBILE INCUSTODITO.
- CRITTOGRAFARE IL LAPTOP ED I SUPPORTI ESTERNI CHE CONTENGONO DATI RISERVATI O SENSIBILI.
- ASSICURARSI DI ESEGUIRE FREQUENTEMENTE IL BACKUP DEI DATI.
- ASSICURARSI CHE L'ACCESSO AL DISPOSITIVO MOBILE SIA PROTETTO CON UN PASSCODE E UTILIZZARE LE IMPOSTAZIONI DI CRITTOGRAFIA INTEGRATE PER GARANTIRE LA SICUREZZA DEL DATO IN CASO DI SMARRIMENTO O FURTO DEL DISPOSITIVO.
- CONSIDERARE L'UTILIZZO DI UNA FUNZIONE DI TRACCIAMENTO/CANCELLAZIONE REMOTA, SE SUPPORTATA. AD ES. PER I DISPOSITIVI IOS, ICLOUD FORNISCONO GRATUITAMENTE IL SERVIZIO «TROVA IL MIO IPHONE». ANCHE ANDROID E ALTRI SISTEMI OPERATIVI MOBILI HANNO FUNZIONALITÀ SIMILI.

BEST PRACTICES

MANTENERE LA RISERVATEZZA

PRINCIPIO DEL "WHO HAVE A NEED TO KNOW". CONDIVIDERE LE INFORMAZIONI SENSIBILI SOLO CON CHI NE HA IL TITOLO A RICEVERLE E A TRATTARLE.



CRITTOGRAFARE I MESSAGGI (COME E-MAIL E SIMILI) CHE CONTENGONO INFORMAZIONI SENSIBILI O CHE DEVONO RIMANERE RISERVATE PER CHI NON HA TITOLO A RICEVERLE E TRATTARLE

BEST PRACTICES

STRATEGIE E PIANI PER GESTIRE EVENTI INASPETTATI

È FONDAMENTALE AVERE:

- UN PIANO DI DISASTER RECOVERY E PIÙ IN GENERALE DI BUSINESS CONTINUITY QUALORA SI VERIFICASSE UN EVENTO DANNOSO
- UN INSIEME DI PROCEDURE PER LA MIGRAZIONE DEI SERVIZI E DEI DATI E INOLTRE DI RECUPERO DEI DATI E DELLE OPERAZIONI SVOLTE

SEGNALARE IMMEDIATAMENTE LA PERDITA, LO SMARRIMENTO O IL FURTO DI DISPOSITIVI QUALI WORKSTATION, COMPUTER, MEMORIE DI MASSA, MEMORIE PORTATILI, SERVER, ... APPARTENENTI ALL'ORGANIZZAZIONE PERCHÉ SICURAMENTE CONTERRANNO DATI RISERVATI O SENSIBILI

BEST PRACTICES

NON CONNETTERSI A RETI WI-FI PUBBLICHE NON PROTETTE DA PASSWORD E NON USARLE PER COMUNICARE O GESTIRE DATI SENSIBILI E CRITICI O PER COLLEGARSI A SERVIZI CHE GESTISCONO DENARO COME BANCHE, SITI DI E-COMMERCE

- **UNA RETE WI-FI PUBBLICA È IN GENERE UNA RETE LIBERAMENTE ACCESSIBILE E CON BASSE O NULLE MISURE DI SICUREZZA**
- **E' PRESENTE GENERALMENTE NEGLI HOTEL, COFFEE SHOP, LIBRERIE, AREOPORTI, STAZIONI,…**

SI PUÒ AUMENTARE LA RISERVATEZZA RICORRENDO AD UN SERVIZIO DI RETE PRIVATA VIRTUALE (VPN), ANCHE GRATUITO (ES. PROTON VPN)

DISABILITARE LA CONDIVISIONE DI FILE NON PERMETTE A TERZI DI ACCEDERE AI FILE SUL PROPRIO DISPOSITIVO.

BEST PRACTICES

ALTRO …

USARE I TOOL DI PROTEZIONE CONTRO LE MINACCE CYBER (ANTIVIRUS, FIREWALL, INTRUSION DETECTION SYSTEM E INTRUSION PREVENTIOIN SYSTEM, PROXY FILTER, …) E SOPRATTUTTO NON DISATTIVARLI MAI

FONTE: https://ercicion.altervista.org/blog/?p=3506

NON ALLONTANARSI DALLA POSTAZIONE DI LAVORO SENZA PRIMA AVER BLOCCATO LA PROPRIA WORKSTATION E NON LASCIARE MAI I DISPOSITIVI INCUSTODITI IN LUOGHI PUBBLICI

FONTE: https://www.navigaweb.net/2020/03/postazione-di-smart-working-per.html

EFFETTUARE IL REGOLARE BACKUP DEI DATI

FONTE: https://www.aranzulla.it/che-cose-il-backup-1024295.html

BEST PRACTICES

E ALTRO ANCORA …

- NON CONDIVIDERE INFORMAZIONI PERSONALI O DELL'ORGANIZZAZIONE CON FONTI SCONOSCIUTE, INUSUALI O DI CUI NON CI SI PUÒ FIDARE
- SCARICARE DATI (FILE, PROGRAMMI, …) SOLO DA FONTI SICURE E VERIFICATE
- RIFLETTERE BENE PRIMA DI ABBINARE UN ACCOUNT DI UN SITO O SERVIZIO DI E-COMMERCE CON I DATI DEI PROPRI CONTI BANCARI O CARTE. L'ABBINAMENTO RENDERÀ LE TRANSAZIONI PIÙ VELOCI, MA LA SICUREZZA DI QUESTE SI BASA SOLO SULLE MISURE DI SICUREZZA DEL SITO
- NON FORNIRE AMPIE FUNZIONALITÀ O PERMESSI ALLE APP PRESENTI SUI DISPOSITIVI SE NON STRETTAMENTE NECESSARIO E CONTROLLARE ATTENTAMENTE QUALI DI QUESTI È RAGIONEVOLE CONCEDERE.

FONTE: https://www.leadershipmanagementmagazine.com/articoli/la-comunicazione-duale-capo-e-collaboratore/

FONTE: https://www.kaspersky.it/blog/android-app-security/14233/

FONTE: https://blog.osservatori.net/it_it/pagamenti-e-commerce

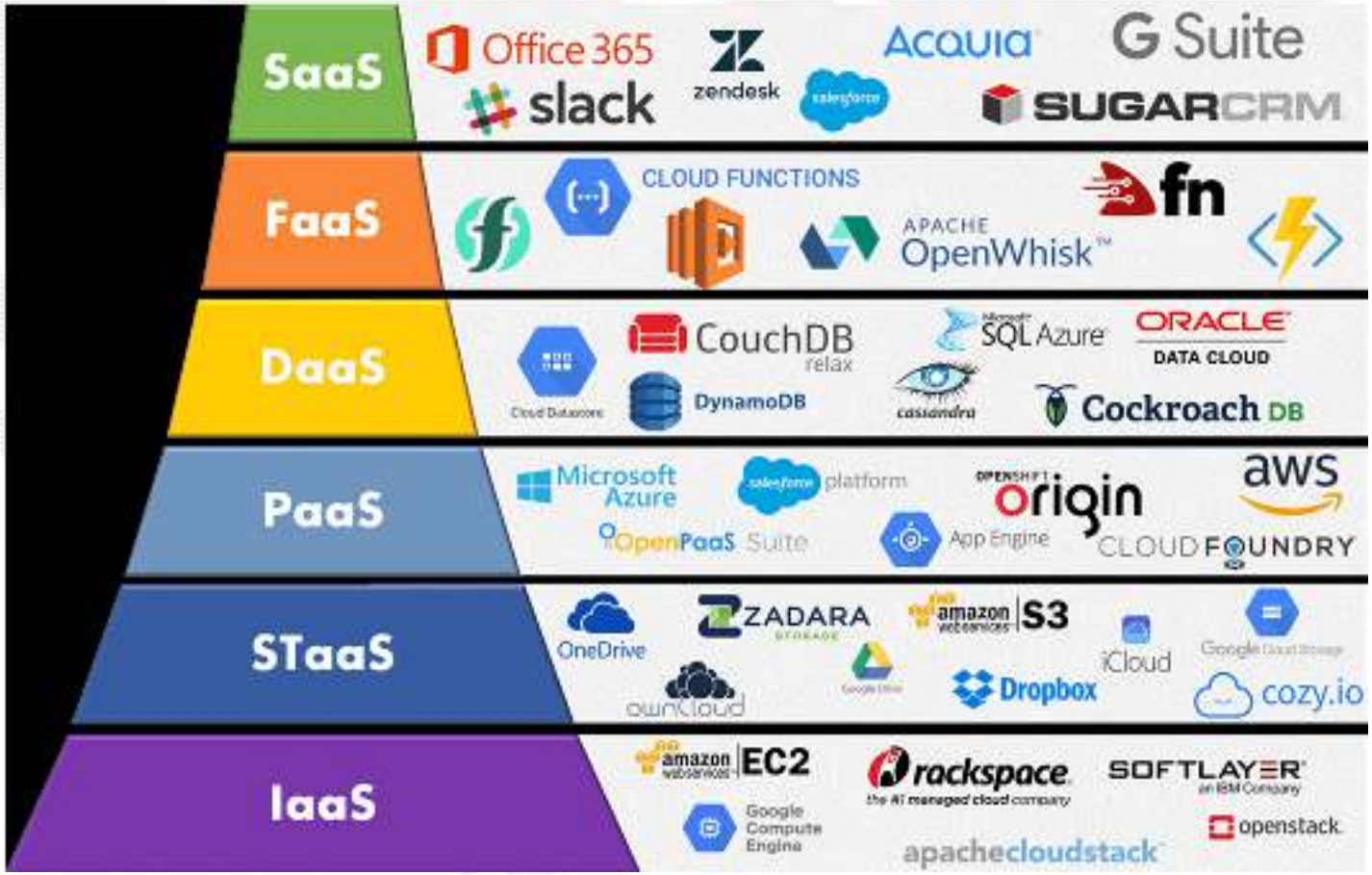
https://tecnologia.libero.it/permessi-e-autorizzazioni-app-android-a-cosa-servono-12040

BEST PRACTICES

PER RIDURRE I RISCHI DI DATA BREACH SI PUÒ RICORRERE AI SERVIZI DI CLOUD COMPUTING

FONTE: https://eduinpro.com/blog/what-is-cloud-computing/

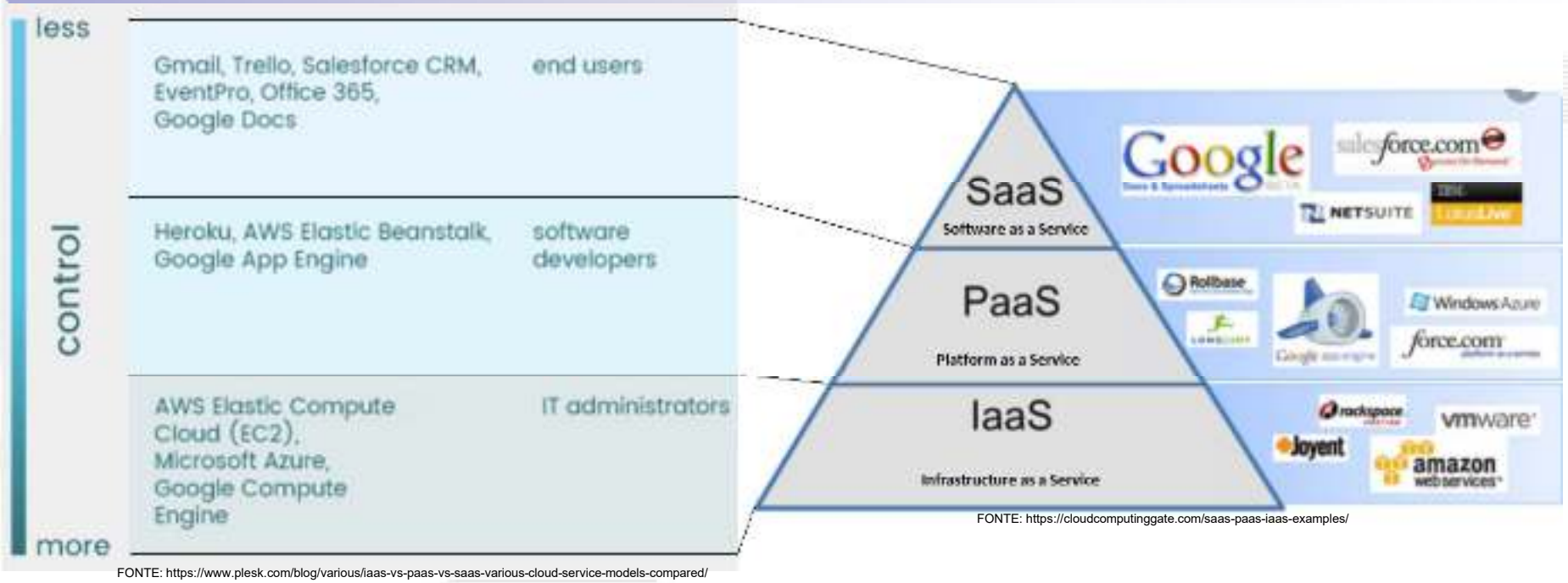
https://linxnet.com.ng/blog/cloud-computing-tips-for-public-sectors/



FONTE: https://kinsta.com/it/blog/google-cloud-vs-aws/

BEST PRACTICES

ALCUNI SERVIZI DEL CLOUD E CARATTERISTICHE



FONTE: https://www.plesk.com/blog/various/iaas-vs-paas-vs-saas-various-cloud-service-models-compared/

FONTE: https://cloudcomputinggate.com/saas-paas-iaas-examples/

CARATTERISTICHE PRINCIPALI DEI SERVIZI CLOUD

1. MOLTA ATTENZIONE ALLA SICUREZZA FISICA E LOGICA ED ALL'AGGIORNAMENTO DELLE PIATTAFORME
2. MAGGIORE GARANZIA DI CONFORMITÀ AGLI STANDARD
3. MAGGIORE RESILIENZA ALLE MINACCE E GESTIONE DELLE VIOLAZIONI DEI DATI

BEST PRACTICES

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

- SONO APPLICATIVI CHE REGISTRANO TUTTE LE OPERAZIONI CHE AVVENGONO NELL'INTERO SISTEMA INFORMATIVO AZIENDALE, IN MODO DA POTER ANALIZZARE, IN TEMPO REALE O A POSTERIORI, GLI EVENTI CHE SI SONO PRESENTATI
- NEL CASO DI ANALISI IN TEMPO REALE, VENGONO GENERATI ALLARMI IN CASO DI EVENTI ANOMALI, RICONDUCIBILI ANCHE A POSSIBILI ATTACCHI CYBER

È IMPORTANTISSIMO AVVALERSI DI STRUMENTI CHE EFFETTUANO PERIODICAMENTE IL BACKUP DEI DATI E DELLE OPERAZIONI SVOLTE (LOGGING).

FONTE: https://www.geekpress.it/come-evitare-di-perdere-il-backup-della-tua-azienda/


Grazie per l'attenzione