Co-funded by the Erasmus+ Programme of the European Union

uli di formazione InCyT

Sicurezza delle informazioni per manager Unità-2 Settimana-3 Nome dell'unità: Gestione della sicurezza delle informazioni -1	
Attività di apprendimento	❑ **Webinar** ❑ **Esercizi** ❑ **Workshop** ❑ **Presentazione** ❑ **Altro** Webinar in streaming, testo, esercizi di autovalutazione, esercizi con risposte su forum di discussione e discussione con il formatore/mentore.
Apprendimento responsabile	• Fatma Gökdemir • Ali Gökdemir
Obiettivi dell'attività di apprendimento	1. Sicurezza delle informazioni 2. Politiche di sicurezza delle informazioni 3. Ruoli di sicurezza informatica
Competenze da acquisire	• IS 1 • IS 3 • SM 3
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?*** • Competenze informatiche intermedie

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brevi informazioni sul modulo

Descrizione
La sicurezza delle informazioni è di grande importanza per garantire la continuità di ogni organizzazione e assicura la protezione delle informazioni critiche dell'organizzazione e di altre risorse informative in vari ambienti, soprattutto quelli elettronici. Non solo le grandi aziende, le holding, ma anche le PMI, le agenzie governative, qualsiasi organizzazione no-profit, le scuole o le persone sole si trovano costantemente a dover affrontare problemi e rischi legati alla sicurezza delle informazioni, anche se a livelli diversi. Negli investimenti per far fronte a questi rischi, la soluzione più costosa e più complessa non è sempre la più sicura. Ogni persona o organizzazione deve scegliere e implementare la soluzione più appropriata e corretta. Non bisogna dimenticare che se una soluzione di sicurezza semplice e a basso costo può essere insufficiente per alcune istituzioni, la stessa soluzione può essere sufficiente ed efficace per un'altra istituzione. Tuttavia, la sicurezza delle informazioni non è un lavoro da iniziare e finire. La gestione della sicurezza delle informazioni è un ciclo di vita che deve essere costantemente gestito e verificato finché esistono istituzioni e informazioni. In questo modulo si spiegherà il concetto di sicurezza delle informazioni, la sua importanza e cosa si deve fare per la sicurezza delle informazioni. L'argomento è supportato da un esempio pratico

Contenuto del materiale didattico

1. Sicurezza delle informazioni

La sicurezza delle informazioni consiste nel prevenire l'accesso, l'uso, la modifica, la divulgazione, la distruzione, la sostituzione e il danneggiamento non autorizzati o non consentiti delle informazioni. Si compone di tre elementi di base chiamati Riservatezza, Integrità e Accessibilità (Figura 1). Se uno di questi tre elementi di base viene danneggiato, si verifica una vulnerabilità della sicurezza.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

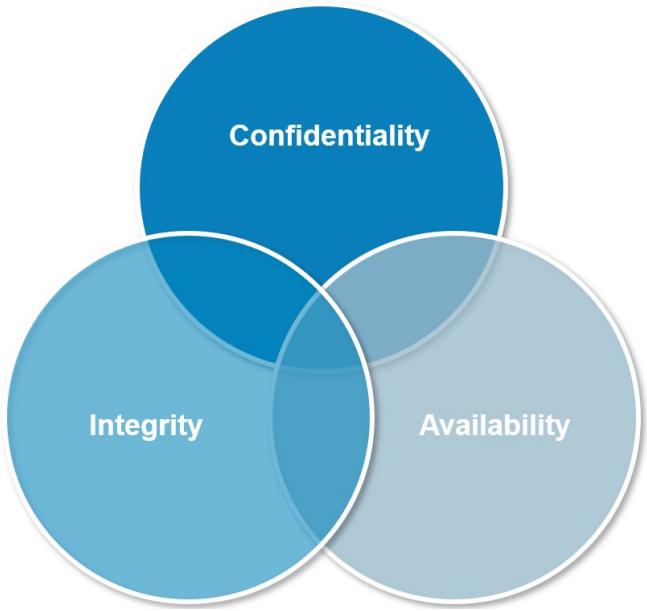


Figura 1. Elementi di sicurezza delle informazioni

- Riservatezza: È la protezione delle informazioni da accessi non autorizzati e da accessi non consentiti.
- Integrità: Le informazioni non vengono modificate da persone non autorizzate.
- Accessibilità: Le informazioni sono accessibili e utilizzabili quando necessario dalle persone autorizzate.

1.1. Che cos'è una policy di sicurezza delle informazioni?

Le minacce alla sicurezza sono in continua evoluzione e i requisiti di conformità diventano sempre più complessi. Le organizzazioni devono creare una policy di sicurezza informatica completa per affrontare entrambe le sfide. Una policy di sicurezza delle informazioni (ISP) è un insieme di regole, politiche e procedure progettate per garantire che tutti gli utenti finali e le reti di un'organizzazione soddisfino i requisiti minimi di sicurezza informatica e di protezione dei dati. Una policy di sicurezza delle informazioni consente di coordinare e applicare un programma di sicurezza e di comunicare le misure di sicurezza a terzi e a revisori esterni.

1.2. Qual è lo scopo di una policy di sicurezza delle informazioni?

Una policy di sicurezza delle informazioni mira a implementare le protezioni e a limitare la distribuzione dei dati solo a chi è autorizzato ad accedervi. Le organizzazioni creano gli ISP per:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Stabilire un approccio generale alla sicurezza delle informazioni
- Documentare le misure di sicurezza e le politiche di controllo dell'accesso degli utenti
- Rilevare e ridurre al minimo l'impatto delle risorse informative compromesse, come l'uso improprio di dati, reti, dispositivi mobili, computer e applicazioni.
- Proteggere la reputazione dell'organizzazione
- Rispettare i requisiti legali e normativi come ENISA, NIST, GDPR, HIPAA e FERPA.
- Proteggere i dati dei clienti, come i numeri delle carte di credito.
- Fornire meccanismi efficaci per rispondere a reclami e domande relative a rischi reali o percepiti di sicurezza informatica come phishing, malware e ransomware
- Limitare l'accesso alle risorse informatiche chiave a coloro che hanno un utilizzo accettabile.

1.3. Perché è importante una policy di sicurezza delle informazioni?

La creazione di una policy di sicurezza delle informazioni efficace e che soddisfi tutti i requisiti di conformità è un passo fondamentale per prevenire incidenti di sicurezza come fughe e violazioni di dati.

Gli ISP sono importanti per le organizzazioni nuove e consolidate. La crescente digitalizzazione significa che ogni dipendente genera dati e una parte di questi dati deve essere protetta da accessi non autorizzati. A seconda del settore, possono essere protetti anche da leggi e regolamenti.

I dati sensibili, le informazioni di identificazione personale (PII) e la proprietà intellettuale devono essere protetti con standard più elevati rispetto agli altri dati.

Che vi piaccia o no, la sicurezza delle informazioni (InfoSec) è importante a tutti i livelli dell'organizzazione. E al di fuori dell'organizzazione.

Le politiche di sicurezza delle informazioni possono avere i seguenti vantaggi per un'organizzazione:

- **Le** politiche di sicurezza delle informazioni standardizzano regole e processi che proteggono da vettori che minacciano l'integrità**, la disponibilità e la** riservatezza dei **dati.**
- **Protezione dei dati sensibili - Le** politiche di sicurezza delle informazioni danno priorità alla protezione della proprietà intellettuale e dei dati sensibili, come le informazioni di

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

identificazione personale (PII).

- **Riduce al minimo il rischio di incidenti di sicurezza -** Una policy di sicurezza delle informazioni aiuta le organizzazioni a definire le procedure per identificare e ridurre le vulnerabilità e i rischi. Inoltre, fornisce risposte rapide per ridurre al minimo i danni in caso di incidenti di sicurezza.
- **Esegue i programmi di sicurezza in tutta l'organizzazione - Le** politiche di sicurezza delle informazioni forniscono il quadro di riferimento per l'operatività delle procedure.
- **Fornisce una chiara dichiarazione di sicurezza alle terze parti** - Le politiche di sicurezza delle informazioni riassumono la posizione di sicurezza dell'organizzazione e spiegano come l'organizzazione protegge le risorse e gli asset IT. Facilitano la risposta rapida alle richieste di informazioni da parte di clienti, partner e revisori.
- **Aiuta a soddisfare i requisiti normativi** - La creazione di una policy di sicurezza delle informazioni può aiutare le organizzazioni a identificare le lacune di sicurezza relative ai requisiti normativi e ad affrontarle.

1.4. Cosa deve contenere una policy di sicurezza informatica?

Una policy di sicurezza delle informazioni può essere difficile da costruire da zero; deve essere solida e proteggere l'organizzazione da tutti i punti di vista. Deve coprire tutti i software, l'hardware, i parametri fisici, le risorse umane, le informazioni e il controllo degli accessi. Deve inoltre essere flessibile e avere spazio per revisioni e aggiornamenti e, soprattutto, deve essere pratica e applicabile. I desideri non vi aiuteranno nello sviluppo di una policy di sicurezza delle informazioni. È necessario collaborare con le principali parti interessate per sviluppare una policy che sia adatta alla vostra azienda e ai dipendenti che saranno responsabili della sua attuazione.

1. ***Policy di utilizzo accettabile***

Questa policy definisce l'uso accettabile delle apparecchiature informatiche e di Internet presso la vostra organizzazione. L'uso improprio di Internet o dei computer espone l'azienda a rischi quali l'attacco di virus, la compromissione dei sistemi e dei servizi di rete e a problemi di natura legale, per cui è importante mettere per iscritto ciò che è o non è accettabile.
Una policy di utilizzo accettabile deve indicare quali sono le responsabilità dei dipendenti per quanto riguarda la protezione delle apparecchiature aziendali, come ad esempio chiudere a chiave i computer quando non sono alla scrivania o salvaguardare i tablet o altri dispositivi elettronici che potrebbero contenere informazioni sensibili. Deve inoltre indicare quali sono i diritti dell'azienda e quali attività non sono vietate sulle apparecchiature e sulla rete aziendale.

2. ***Policy di pulizia della scrivania***

Una policy di pulizia delle scrivanie si concentra sulla protezione delle risorse fisiche e delle

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

informazioni. Idealmente, questa policy garantirà che tutti i materiali sensibili e riservati siano chiusi a chiave o messi in sicurezza in altro modo quando non vengono utilizzati o quando un dipendente lascia la propria scrivania. Questa policy deve stabilire i requisiti minimi per mantenere una scrivania pulita, come ad esempio dove possono essere archiviate e accessibili le informazioni sensibili sui dipendenti, la proprietà intellettuale, i clienti e i fornitori. Dovrebbe inoltre indicare quali tipi di materiali devono essere distrutti o gettati via, se è necessario utilizzare una password per recuperare i documenti da una stampante e quali informazioni o proprietà devono essere protette con un lucchetto fisico. Oltre a essere una parte comune e importante di qualsiasi policy di sicurezza delle informazioni, una policy di clean desk è conforme alla norma ISO 27001/17799 e aiuterà la vostra azienda a superare un audit di certificazione.

3. ***Policy di risposta alle violazioni dei dati***

Si tratta anche di un piano di risposta agli incidenti. Lo scopo di una policy di risposta alla violazione dei dati è quello di stabilire gli obiettivi e la visione di come l'organizzazione risponderà a una violazione dei dati. Questo piano aiuterà a mitigare i rischi di essere vittima di un attacco informatico, perché descriverà in dettaglio come l'organizzazione intende proteggere le risorse di dati durante il processo di risposta all'incidente.

Questa policy deve definire a chi si applica e quando entra in vigore, compresa la definizione di violazione, i ruoli e le responsabilità del personale, gli standard e le metriche, i meccanismi di segnalazione, di rimedio e di feedback.

4. ***Policy del piano di ripristino di emergenza***

Questa policy è diversa da un piano di risposta alle violazioni dei dati perché si tratta di un piano di emergenza generale per le azioni da intraprendere in caso di disastro o di qualsiasi evento che provochi un ritardo prolungato del servizio. Questa policy deve descrivere il processo di recupero dei sistemi, delle applicazioni e dei dati durante o dopo qualsiasi tipo di disastro che provochi un'interruzione importante. Il piano di disaster recovery deve essere aggiornato annualmente.

Il piano di emergenza deve comprendere questi elementi:

- Piano di emergenza. Elencate esplicitamente chi deve essere contattato, quando deve essere contattato e come lo farete?
- Piano di successione. Descrivere il flusso di responsabilità quando il personale normale non è in grado di svolgere le proprie mansioni.
- Piano di classificazione dei dati. Dettagliare tutti i dati memorizzati su tutti i sistemi, la loro criticità e la loro riservatezza.
- Elenco dei servizi critici. Elencare tutti i servizi forniti e il loro ordine di importanza.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Piano di backup e ripristino dei dati. Descrivete in dettaglio quali dati vengono sottoposti a backup, dove e con quale frequenza. Spiegate anche come è possibile ripristinare i dati.
- Piano di sostituzione delle apparecchiature. Descrivere quali servizi infrastrutturali sono necessari per riprendere a fornire servizi ai clienti.
- Comunicazioni pubbliche. Documentate chi sarà il responsabile della funzione di pubbliche relazioni esterne e fornite linee guida su quali informazioni possono e devono essere condivise.
- È importante che il team di gestione dedichi del tempo a testare il piano di ripristino d'emergenza. Durante questi test, noti anche come esercitazioni su tavolo, l'obiettivo è identificare i problemi che potrebbero non essere evidenti nella fase di pianificazione e che potrebbero causare il fallimento del piano. In questo modo, il team può adeguare il piano prima che si verifichi un disastro.

5. *Policy di posta elettronica*

La posta elettronica è un canale di comunicazione fondamentale per le aziende di tutti i tipi e il suo uso improprio può rappresentare una minaccia per la sicurezza della vostra azienda, sia che si tratti di dipendenti che usano la posta elettronica per distribuire informazioni riservate o che espongano inavvertitamente la vostra rete a un virus. È importante che tutti i dipendenti, gli appaltatori e gli agenti che operano per conto della vostra azienda comprendano l'uso appropriato della posta elettronica e dispongano di politiche e procedure per archiviare, contrassegnare e rivedere le e-mail quando necessario.

Questa policy deve delineare l'uso appropriato degli indirizzi di posta elettronica aziendali e coprire aspetti quali i tipi di comunicazione vietati, gli standard di sicurezza dei dati per gli allegati, le regole di conservazione delle e-mail e l'eventuale monitoraggio delle e-mail da parte dell'azienda. Questa policy deve essere chiaramente definita anche per i dipendenti, in modo che comprendano la loro responsabilità nell'uso dei loro indirizzi e-mail e la responsabilità dell'azienda nell'assicurarsi che le e-mail siano usate correttamente. Questa policy di gestione della posta elettronica non serve a creare una policy "a prova di bomba" per catturare i dipendenti che fanno un uso improprio della posta elettronica, ma a evitare una situazione in cui i dipendenti fanno un uso improprio della posta elettronica perché non capiscono cosa è e cosa non è consentito.

6. *Policy di protezione della chiave di crittografia dell'utente finale*

Alcuni documenti e comunicazioni all'interno dell'azienda o distribuiti agli utenti finali potrebbero dover essere crittografati per motivi di sicurezza. È necessario adottare una policy per la protezione delle chiavi di crittografia, in modo che non vengano divulgate o utilizzate in modo fraudolento.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Questa policy deve delineare tutti i requisiti per la protezione delle chiavi di crittografia ed elencare i controlli operativi e tecnici specifici per mantenerle al sicuro. Tra questi figurano elementi come l'hardware resistente alle manomissioni, le procedure di backup e le azioni da intraprendere nel caso in cui una chiave di crittografia venga persa, rubata o utilizzata in modo fraudolento.

7. Policy di protezione della password

I vostri dipendenti hanno probabilmente una miriade di password che devono tenere sotto controllo e utilizzare quotidianamente, e la vostra azienda dovrebbe avere standard chiari ed espliciti per la creazione di password forti per i loro computer, account di posta elettronica, dispositivi elettronici e qualsiasi punto di accesso ai vostri dati o alla vostra rete.

Questa policy deve anche delineare ciò che i dipendenti possono o non possono fare con le loro password. Potrebbe sembrare ovvio che non debbano inserire le loro password in un'e-mail o condividerle con i colleghi, ma non dovete dare per scontato che sia una conoscenza comune per tutti. Fornite ai vostri dipendenti tutte le informazioni necessarie per creare password forti e tenerle al sicuro per ridurre al minimo il rischio di violazione dei dati.

Infine, questa policy dovrebbe delineare ciò che gli sviluppatori e il personale IT devono fare per assicurarsi che tutte le applicazioni o i siti web gestiti dall'azienda seguano le precauzioni di sicurezza per mantenere le password degli utenti al sicuro.

Le ricerche condotte nell'ultimo decennio in tutto il mondo mostrano che le password preferite dagli utenti sono le seguenti:

- 123456
- password
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Nonostante gli avvertimenti annuali, questo elenco non è cambiato molto. Per questo motivo, si consiglia agli utenti di seguire una serie di regole di impostazione delle password. Queste regole sono elencate di seguito:

- Impostazione dei requisiti di complessità, come il rispetto del requisito di carattere minimo
- Non scegliere le password usate in precedenza

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Cambiare le password periodicamente e magari frequentemente
- Le password utilizzate non devono essere scelte tra quelle comuni e debolmente utilizzate, come nell'elenco precedente.

Il National Institute of Standards and Technology (NIST) si è posto l'obiettivo di risolvere il problema delle politiche sulle password per determinarle e raggiungere determinati standard. Il NIST definisce i dettagli sulle password e su come devono essere gestite e conservate. Di conseguenza, le possibili password devono essere verificate rispetto a un elenco di valori comunemente utilizzati e conosciuti. Le considerazioni per la determinazione delle password sono le seguenti:

- Le password fornite dall'utente devono essere composte da almeno otto caratteri alfanumerici.
- Non devono essere password ottenute da precedenti violazioni.
- Non ci dovrebbero essere parole da dizionario.
- Non devono essere presenti date tra il 1900-2020, come ad esempio le date di nascita.
- Nessun carattere ripetitivo o sequenziale (ad esempio, aaaaaaaa o 1234abcd).
- Non devono essere utilizzate parole specifiche per l'uso previsto, come il nome del servizio, il nome utente e i suoi derivati.

I criteri di cui sopra devono essere presi in considerazione nella determinazione delle password e devono essere create password con strutture complesse.

Complessità della password: la complessità della password è definita come il numero di password che sono forti per una password si intende che soddisfa una serie di regole. La chiave della complessità delle password Le regole sono le seguenti:

- La password non può contenere il nome dell'account o sue variazioni.
- La password deve contenere sia lettere maiuscole (A-Z) sia lettere minuscole (a-z).
- Caratteri speciali **(~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)** (Questi sono i caratteri che di solito vengono visualizzati con il tasto ALT. Tuttavia, i simboli di valuta come l'euro non sono considerati caratteri speciali).
- Il numero minimo di caratteri deve essere rispettato. Questo valore varia da sistema a sistema e da utente a utente. può cambiare.

La lunghezza minima della password deve essere di 8 caratteri, mentre quella consigliata è di 12 caratteri.

Quando le password sono create con almeno 8 caratteri secondo le regole sopra elencate, ciò significa almeno 218.340.105.584.896 possibilità diverse per una singola password. La probabilità della password generata rende molto difficile un attacco di forza bruta, ma la password non è ancora impossibile da decifrare. Per una password quasi impossibile da decifrare, è necessario aumentare il numero di caratteri della password. Più alto è il numero minimo di caratteri, più tempo è necessario per decifrare la password.

Oltre ai vantaggi della complessità delle password, essa comporta anche alcune sfide. Una delle

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

principali è quella di dimenticare la password. È difficile ricordare una password più lunga e contenente caratteri speciali. Soprattutto quando tutte le password sono diverse, è difficile ricordarle e non confonderle con altre. Pertanto, è necessario seguire una certa logica nella creazione delle password.

Ad esempio;

- **S**ono **i**l **s**econdo **f**iglio **d**i **u**na **f**amiglia **c**on 3 **f**igli**!**

Potete scrivere una frase come questa basandovi sulla vostra vita reale. Prendendo i primi caratteri e i caratteri speciali della frase, si ottiene una password come **Sisfdufc3f!!**

- Sono diventato membro di questo sito web (sull'istruzione) il 19 luglio.

È possibile personalizzare una frase come "**S**ono **d**iventato **m**embro **d**i **q**uesto **s**ito **w**eb (**s**ull'**i**struzione) **i**l 19 **l**uglio**!!**" in base all'area di interesse del sito e alla data di iscrizione, in modo da non dimenticarla. Prendendo i primi caratteri e i caratteri speciali della frase, si ottiene una password come **Sdmdqsw(si)i19l!!**

8. Policy del piano di risposta alla sicurezza

Un piano di risposta alla sicurezza stabilisce cosa deve fare ogni team o unità aziendale in caso di incidente di sicurezza, come una violazione dei dati. Secondo il SANS Institute, dovrebbe definire "la descrizione del prodotto, le informazioni di contatto, i percorsi di escalation, gli accordi sul livello di servizio (SLA) previsti, la classificazione della gravità e dell'impatto e le tempistiche di mitigazione/rimedio".

La chiave di una policy del piano di risposta alla sicurezza è che aiuta tutti i diversi team a integrare i loro sforzi in modo che qualsiasi incidente di sicurezza possa essere mitigato il più rapidamente possibile. Mentre ogni reparto può avere i propri piani di risposta, la policy del piano di risposta alla sicurezza descrive in dettaglio come si coordineranno tra loro per assicurarsi che la risposta a un incidente di sicurezza sia rapida e completa.

1.5. Esempi di politiche di sicurezza delle informazioni

Per creare un piano di sicurezza informatica di successo, è necessario considerare 5 aspetti principali.

a. ***Identificare:*** *L*'organizzazione deve avere una comprensione dei rischi di cybersecurity che deve affrontare, in modo da poter dare priorità ai propri sforzi.

b. ***Proteggere***: Si tratta di mettere in atto misure di salvaguardia adeguate per proteggere le risorse di dati e limitare o contenere l'impatto di un potenziale evento di cybersecurity. Ciò include l'educazione e la responsabilizzazione dei membri del personale all'interno dell'organizzazione affinché siano consapevoli dei rischi, la definizione di procedure incentrate sulla protezione della sicurezza

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

della rete e degli asset e l'eventuale utilizzo di un'assicurazione di responsabilità civile informatica per proteggere finanziariamente l'azienda nel caso in cui un criminale informatico sia in grado di eludere le protezioni in atto.

c. ***Rilevare***: Delineare le attività che aiutano a scoprire il verificarsi di un attacco informatico e consentono di reagire tempestivamente all'evento. Per diagnosticare in modo rapido ed efficiente un attacco informatico, le aziende devono implementare protocolli di classificazione dei dati, gestione degli asset e gestione del rischio che le avvisino quando i dati sembrano essere compromessi.

d. ***Rispondere***: Documentare le azioni appropriate da intraprendere in seguito al rilevamento di minacce alla sicurezza informatica. La risposta dell'azienda deve comprendere una comunicazione adeguata e approfondita con il personale, gli azionisti, i partner e i clienti, nonché con le forze dell'ordine e i consulenti legali, se necessario.

e. ***Recuperare***: Determinare come un'organizzazione può recuperare e ripristinare le capacità o i servizi che sono stati compromessi a causa di un attacco informatico.

Quasi tutti gli standard di sicurezza devono includere un requisito per un qualche tipo di piano di risposta agli incidenti, perché anche i piani di sicurezza delle informazioni e i programmi di conformità più solidi possono essere vittime di una violazione dei dati.

1.6. Esercizi della policy di sicurezza delle informazioni

1. Bloccate la vostra sessione: Rafforzate i vostri account online attivando gli strumenti di autenticazione più forti disponibili, come la biometria (tracce biologiche misurabili di una persona), le chiavi di sicurezza o un codice unico generato da uno strumento applicativo sul vostro dispositivo mobile. I vostri nomi utente e le vostre password potrebbero non essere sufficienti per proteggere account come quelli di e-mail, banche e social media.

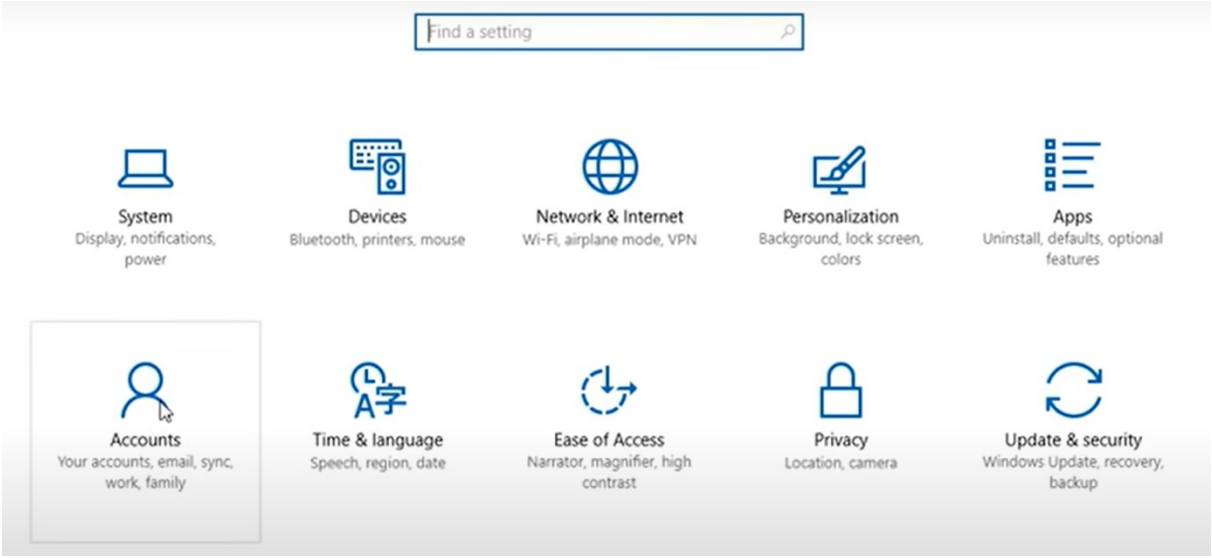
Esercizi-1:

Per far sì che il computer si blocchi automaticamente quando ci si alza dal computer.

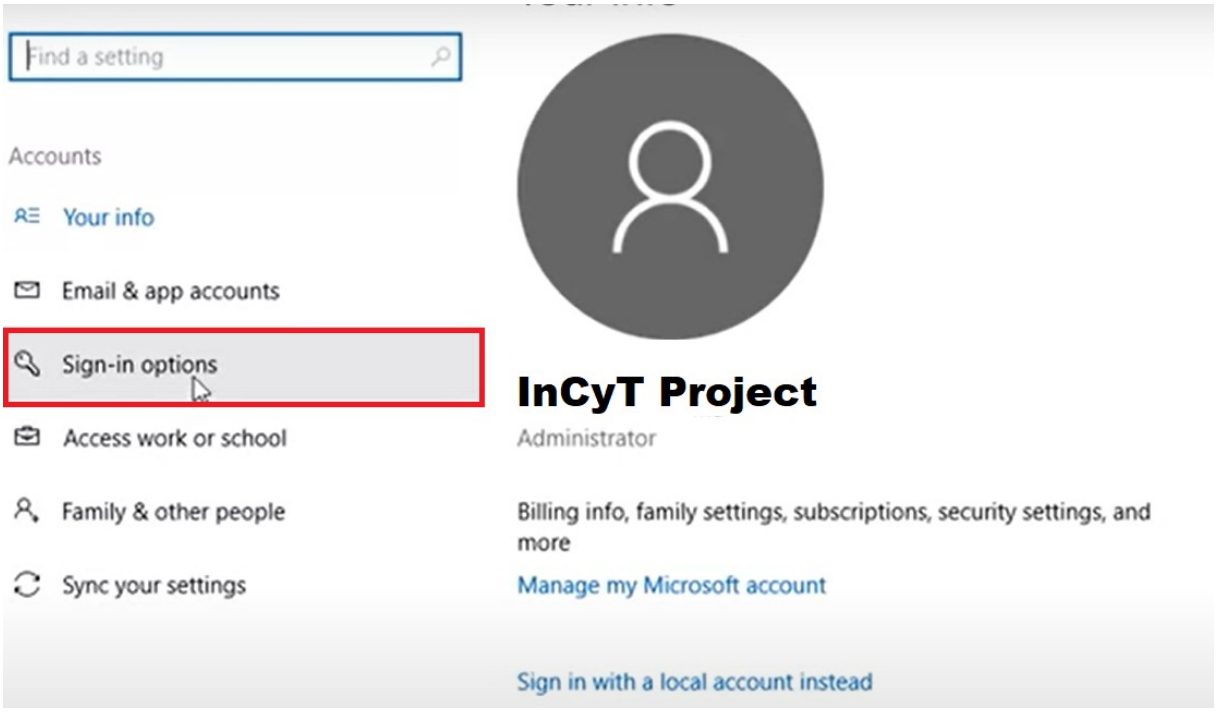
Passo 1: fare clic sul pulsante Impostazioni di Windows.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Fase 2: fare clic sulla scheda Account.



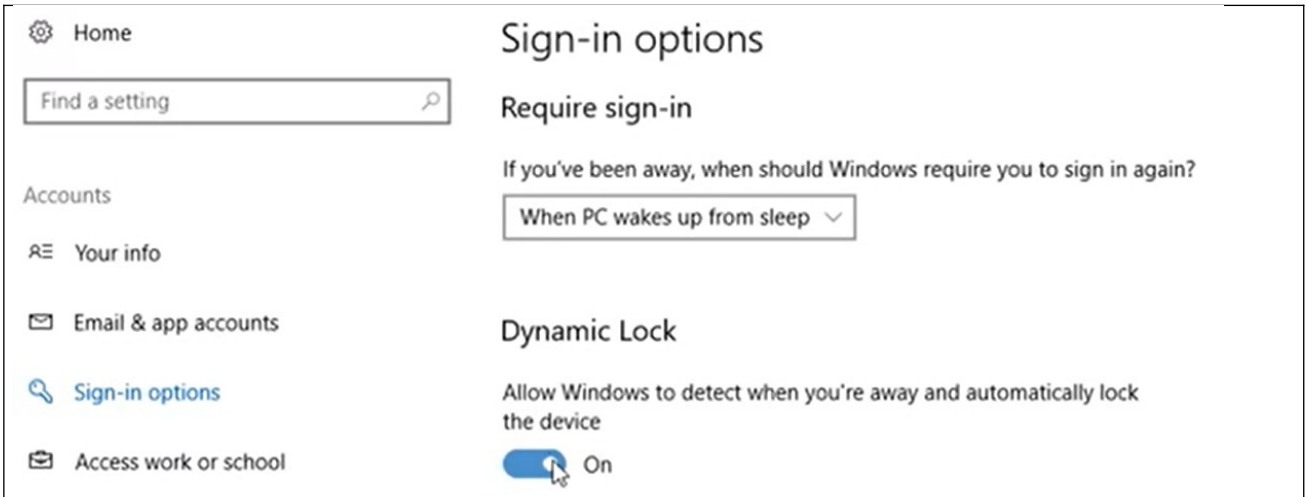
Fase 3: Fare clic sulla sezione Accedi.



Fase 4: Abilitare la funzionalità di blocco dinamico.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



2- Creare una password forte: la password ha un ruolo importante nella sicurezza delle informazioni. Le password deboli possono essere risolte in breve tempo con programmi di cracking delle password. Per questo motivo, è necessario prestare la massima attenzione tenendo conto delle seguenti regole quando si creano e si utilizzano le password su tutti i dispositivi e gli account. La password è generalmente utilizzata in molti punti dei sistemi informatici. La password viene utilizzata per la creazione di un account di posta elettronica, per impostare una password di accesso al computer e per vietare l'accesso ai file. Tuttavia, le password non devono essere deboli o indovinabili. Le password devono essere create secondo i seguenti criteri:

a. Le password devono essere lunghe ***almeno 8 caratteri*** e contenere almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale (.-+=_,!@$#*%<>[]{}).
b. Il campo della password ***non deve essere*** lasciato vuoto o predefinito; ***123456, 01062022, qwerty, password ecc.*** non deve essere determinato in modo tale da essere prevedibile e facilmente violabile come le parole che si possono trovare in qualsiasi dizionario.
c. Le password **non** devono **contenere informazioni personali** (nome del bambino, data di nascita o nome dell'istituto).
d. È necessario creare ***password diverse*** per sistemi e account diversi.
e. Le password devono essere ***cambiate*** frequentemente (almeno ogni 6 mesi).
f. Le password ***non devono essere scritte*** in luoghi che possano essere notati da altre persone (ad esempio lasciandole accanto al computer o scrivendole su carta) e non devono essere memorizzate in chiaro senza crittografia su un computer o su qualsiasi supporto digitale.
g. Nessun dipendente o studente deve ***condividere*** la propria password (password di posta elettronica, password di firma elettronica, password del PC, ecc. Gli utenti devono sapere che tutte le responsabilità legali che possono sorgere in caso di condivisione saranno a loro carico.

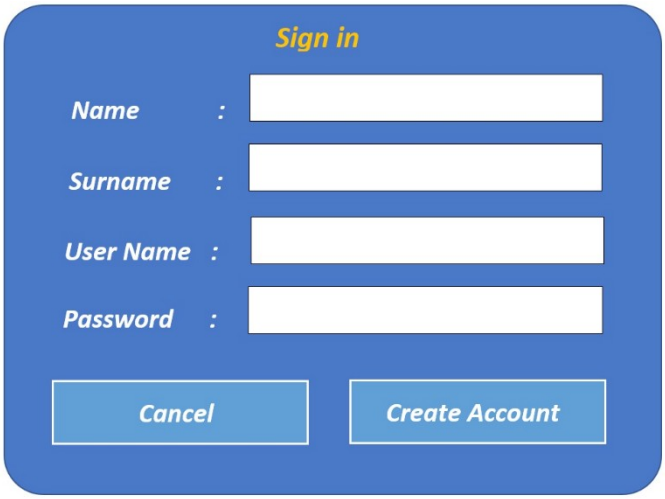
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

h. Account unico, password unica: avere una password separata per ogni account aiuta a contrastare i criminali informatici. Come minimo, separate gli account di lavoro da quelli personali e assicuratevi che i vostri account critici abbiano le password più forti.
i. Ricordatela e tenetela al sicuro: Le password forti sono difficili da creare e ricordare. Impostate le vostre password in modo che siano significative e memorabili solo per voi, oppure conservatele in un luogo e in un formato sicuri. In alternativa, potete utilizzare un servizio come un password manager per tenere traccia delle vostre password.

Esercizi-2:

Sicurezza della password quando si crea un account di posta elettronica tramite il provider di servizi di posta elettronica aziendale o un'applicazione o un sito web di un provider di servizi di posta elettronica pubblico.

Fase 1: aprire il sito web o l'applicazione.
Fase 2: Inserire le informazioni personali per creare un account.



Fase 3: quando si crea una password, utilizzare combinazioni di maiuscole, minuscole, cifre e simboli.
Per rendere la password facile da ricordare da parte dell'utente, si possono eseguire alcune operazioni di codifica. Ad esempio, si può scrivere una frase adatta all'argomento e utilizzare i primi caratteri, i numeri e i caratteri speciali della frase scritta.

Questo progetto di cybersecurity è sostenuto dal programma Erasmus+ 2021.

Fase 4: Impostiamo la nostra password; QpdcsdpE+2021

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Fase 5: Assicurarsi che la password sia composta da almeno 8 caratteri. Sono preferibili 12 caratteri. Si può dire che la password che utilizziamo è adatta perché ha 12 caratteri.

3- Accesso a siti sicuri (Safe Browser): Quando si va online per fare acquisti o leggere notizie, si utilizza un browser. I browser sono uno dei modi principali per interagire con Internet. Di conseguenza, i browser sono i principali obiettivi degli aggressori informatici.
Utilizzate sempre la versione più recente del vostro browser e mantenete il vostro scudo di sicurezza contro gli attacchi informatici. I browser aggiornati dispongono delle ultime patch di sicurezza e sono molto più difficili da sfruttare per i cyber-attaccanti. Non siete sicuri di avere l'ultimo aggiornamento del browser? Contattate il team di assistenza tecnica o il team di sicurezza informatica per verificarlo. Rimanete al sicuro online non collegandovi ai siti web quando ricevete un avviso dal vostro browser.
I browser moderni sono in grado di riconoscere alcuni siti web dannosi che sono progettati per nuocere. Se il browser vi segnala che il sito web che state per visitare è pericoloso, chiudete la pagina web e cercate di trovare le informazioni che state cercando su un sito più sicuro.
Prima di inviare informazioni sensibili online, ad esempio i dati della carta di credito per gli acquisti online, assicuratevi che il vostro browser utilizzi il protocollo HTTPS, che indica la crittografia. La crittografia mescola le informazioni trasmesse tra il vostro computer e la destinazione in modo che solo il sito web autorizzato possa leggerle.
Per una connessione sicura, cercate segni di crittografia come l'indirizzo del sito web che inizia con HTTPS e l'icona di un lucchetto nella barra di stato.

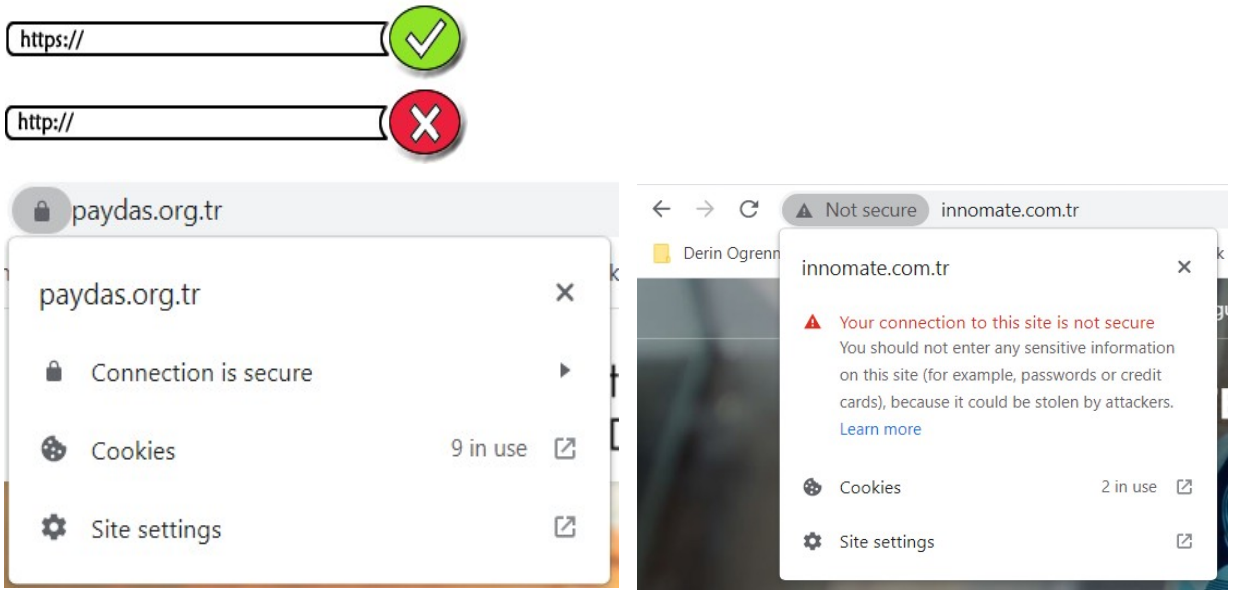


Figura 2. Siti web sicuri e non sicuri

I componenti aggiuntivi sono piccoli pezzi di software aggiunti ai browser che vengono utilizzati per funzioni aggiuntive come giocare, guardare film o modificare testi. Ogni componente

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

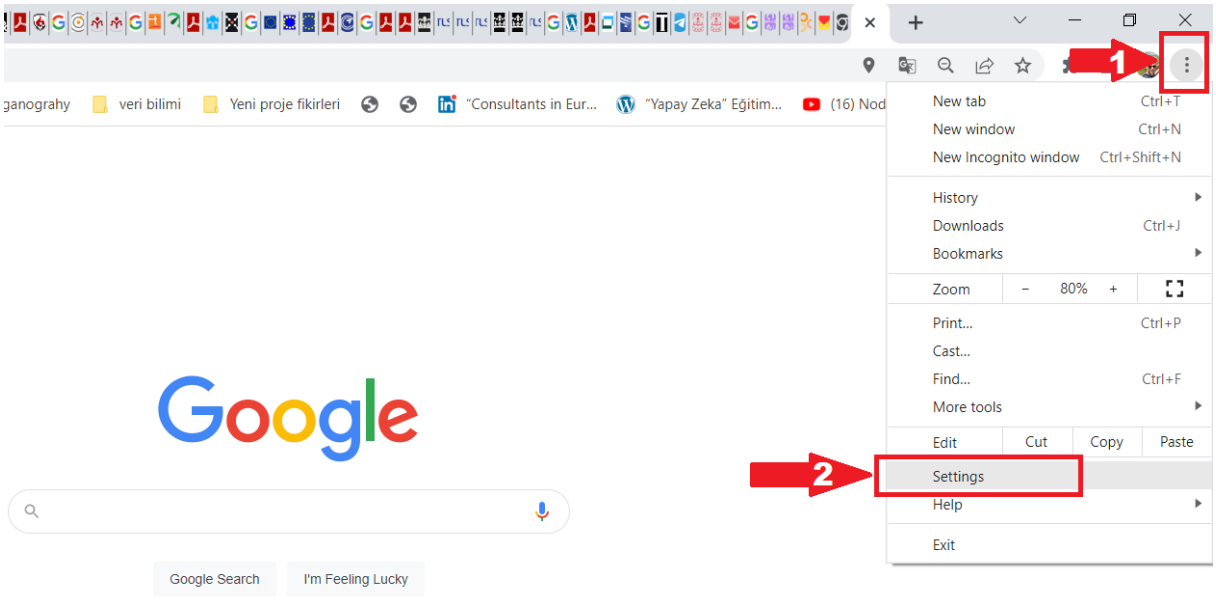
aggiuntivo installato nel browser aggiunge potenzialmente ulteriori vulnerabilità alla sicurezza. Se ne avete assolutamente bisogno e solo previa approvazione, installate i componenti aggiuntivi nel vostro browser. Una volta installati, utilizzate sempre la versione più recente del plugin, proprio come nel vostro browser.

Infine, al termine della visita di un sito web, assicuratevi di aver effettuato il logout. In questo modo si rimuovono le informazioni sensibili di login e password prima di chiudere il browser. Ricordate che il vostro comportamento di navigazione sicura e il vostro scudo di sicurezza sono rafforzati.

Esercizi-3:

Per modificare i plug-in nel browser web, procedere come segue.

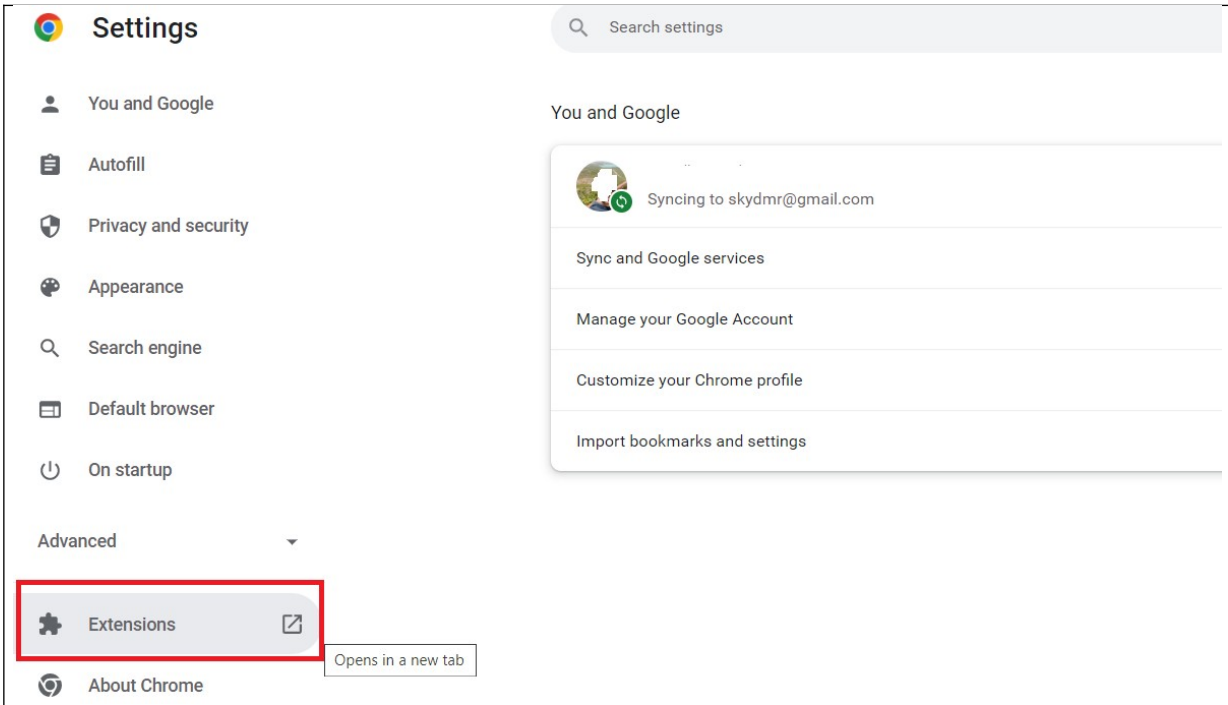
Fase 1: aprire il browser Web e fare clic sul pulsante "Custom control..." nell'angolo superiore destro (1). Fare clic sulla scheda "Impostazioni/Settings" dal menu a discesa (2).



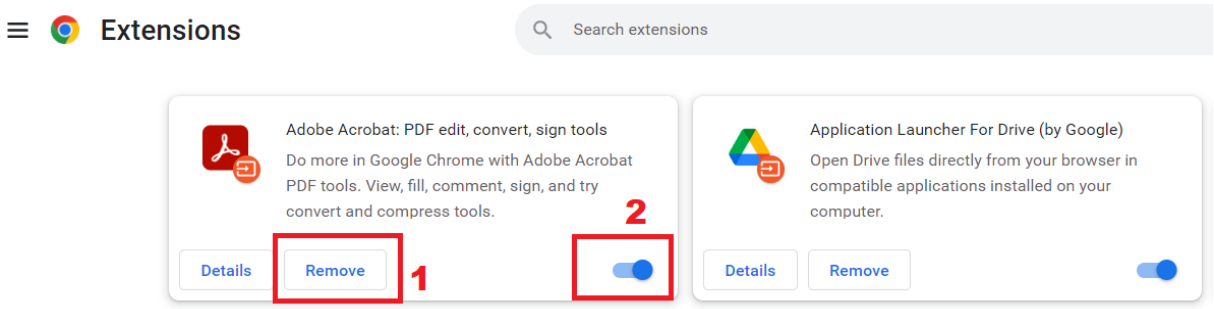
Fase 2: Fare clic sul pulsante "Estensioni" nella finestra che si apre.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Fase 3: In questa schermata è possibile vedere i componenti aggiuntivi installati nel browser. Se si desidera eliminare un componente aggiuntivo, è possibile eliminarlo (1) premendo il pulsante "Rimuovi". Se si desidera che il plugin rimanga inattivo, è possibile disattivarlo dal pulsante "On-Off" (2).



4. Email, messaggistica e phishing: avere un'email nella casella di posta o un messaggio sul telefono. "C'è un problema con il vostro account e il vostro account deve essere aggiornato immediatamente. Tutto ciò che deve fare è cliccare su un link". Quando ricevete un messaggio con un contenuto, fermatevi e pensate prima di cliccare! Il "phishing" è un attacco di ingegneria sociale che utilizza le e-mail o la messaggistica come esca, come le esche per la pesca.
Gli aggressori informatici inviano migliaia di e-mail nella speranza che qualcuno abbocchi. Le e-mail invitano a compiere un'azione, come cliccare su un link, aprire un allegato o compilare un

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

modulo. Gli aggressori informatici non sanno esattamente chi riceverà queste e-mail, ma l'esecuzione di una di queste azioni apparentemente innocue potrebbe farvi abboccare.
Una forma più sofisticata di phishing, chiamata "Spear phishing", prende di mira individui specifici. Ad esempio, quando tutti i membri della nostra organizzazione ricevono un'e-mail generica di phishing relativa a un pacco non consegnato; come cinque persone della nostra unità acquisti che vengono prese di mira con una falsa richiesta di fattura.

Come facciamo a sapere se un'e-mail o un messaggio è un attacco di phishing?
Alcuni segnali da ricercare:

- Messaggi che iniziano con "Gentile cliente" o altre voci di saluto generali.
- Messaggi che richiedono un'azione immediata o che creano un senso di urgenza, come la minaccia di chiudere l'account.
- Messaggi che affermano di provenire da un'organizzazione ufficiale ma che presentano errori grammaticali o di ortografia o che utilizzano un indirizzo e-mail personale come @gmail.com, @yahoo.com o @hotmail.com.
- Qualsiasi messaggio che richieda informazioni altamente sensibili, come il numero della carta di credito o la password. Diffidate di questi messaggi. Se qualcuno che conoscete, ad esempio un collega, vi invia un messaggio che richiede un'azione urgente, contattatelo attraverso diversi canali per verificare che sia davvero lui ad avervi inviato il messaggio, ad esempio con una telefonata Cercate di confermare se il messaggio è suo.

Ricordate che è molto facile per un cyber-attaccante creare un'e-mail che sembri provenire da un amico o da un collega. Per essere sicuri, è necessario adottare sempre le seguenti precauzioni quando si utilizza la posta elettronica o la messaggistica. Passare il mouse su un link prima di cliccarlo. In questo modo si visualizza la vera destinazione del link e si può confermare che si è stati reindirizzati a un sito web legittimo. Ancora meglio è digitare l'indirizzo del sito web direttamente nel browser.
Ad esempio, se ricevete un'e-mail dalla vostra banca che vi chiede di aggiornare i dettagli del conto, ignorate il link inviato via e-mail. Digitate semplicemente l'indirizzo del sito web della vostra banca nel browser e accedete come al solito. Quando i messaggi contengono allegati, aprite solo quelli che vi aspettate.
Poiché le soluzioni antivirus potrebbero non rilevare tutte le versioni di malware, l'utente è la migliore difesa contro gli allegati infetti. Quando utilizzate la posta elettronica o la messaggistica, fate attenzione a non rivelare accidentalmente informazioni importanti.
Le funzioni di posta elettronica come il completamento automatico rendono facile l'invio

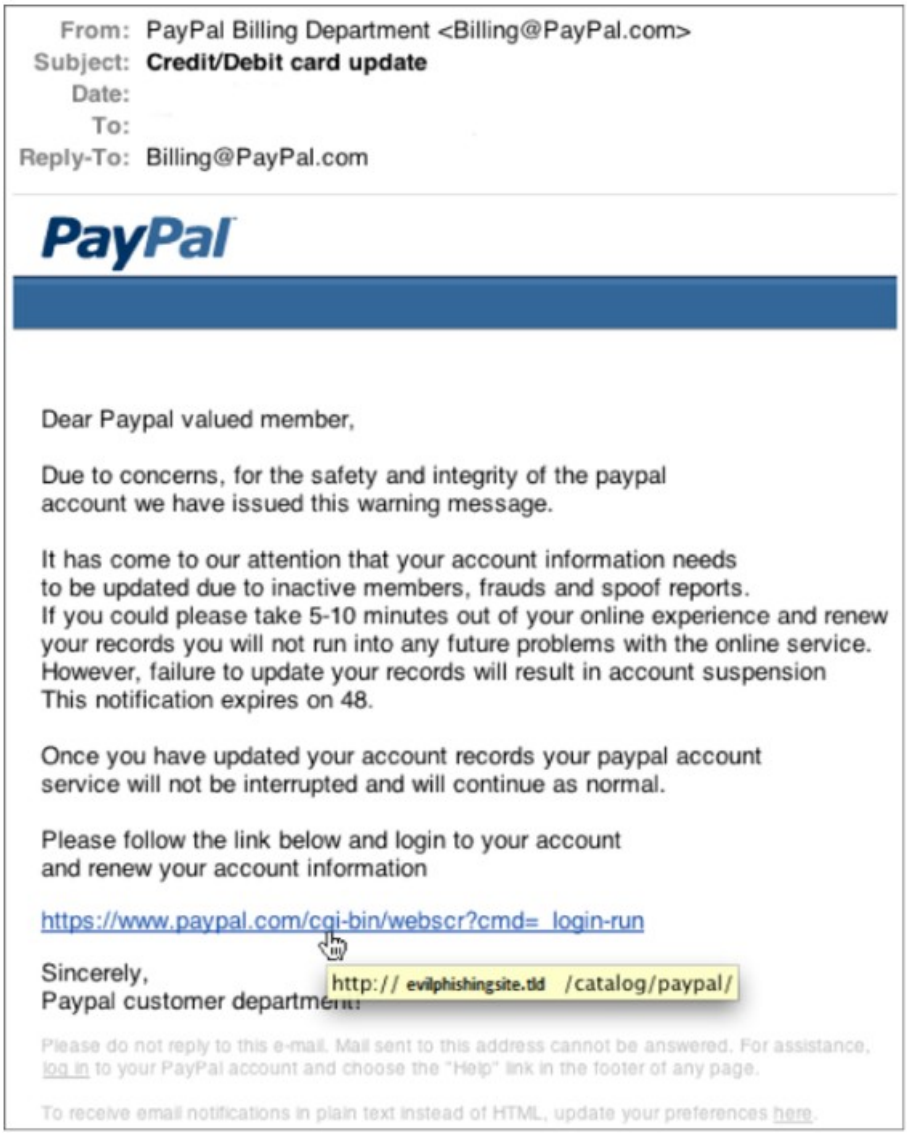
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

involontario di e-mail alla persona sbagliata. Ad esempio, quando si vuole inviare un'e-mail a qualcuno che lavora nella propria unità, si può accidentalmente inviare un'e-mail a un amico con un nome simile che lavora in un'altra unità. Ricordate che una volta inviata un'e-mail è fuori dal vostro controllo.

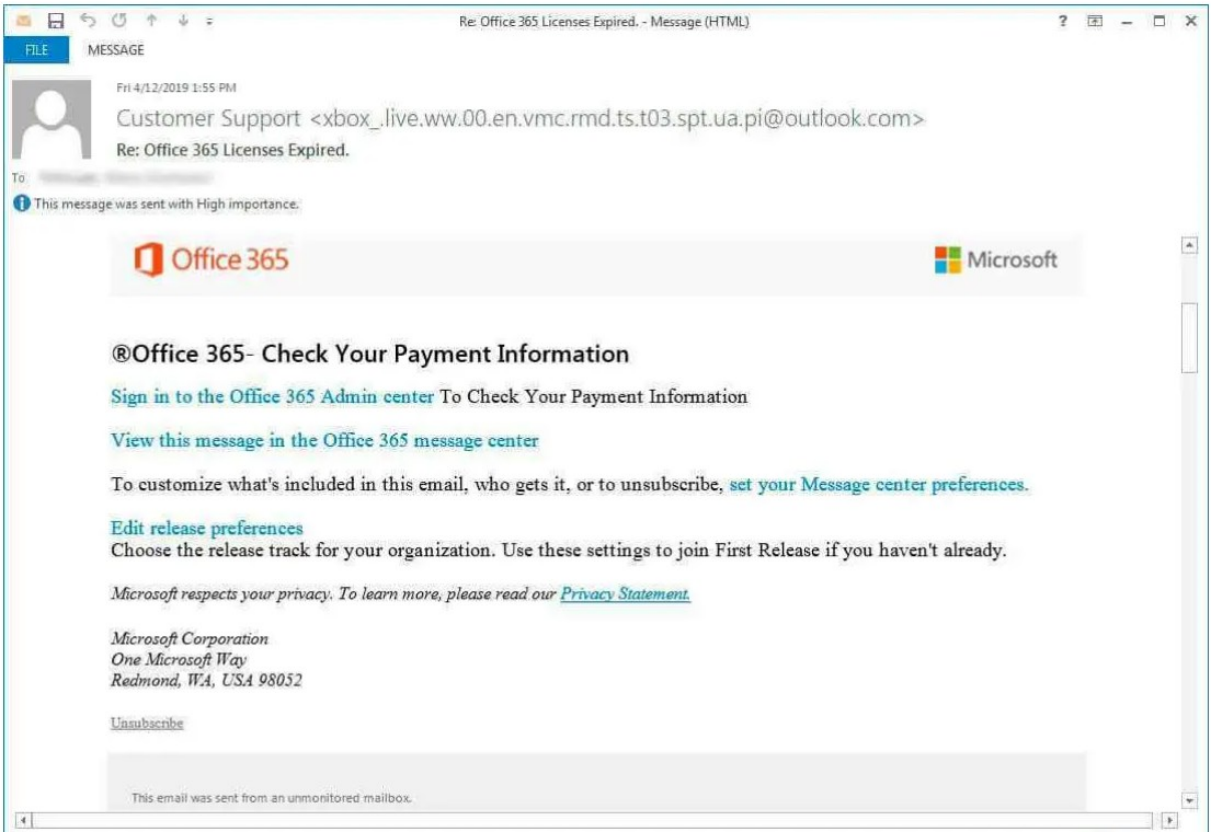
Esempi di phishing

Esempio-1: in questo esempio, l'e-mail sembra inviata da PayPal.com, ma è inviata attraverso un server falso. Se osserviamo solo l'indirizzo web a cui è indirizzata, senza cliccare sul link indicato, possiamo rilevare che si tratta di un'e-mail raccolta da un aggressore che vuole ottenere le credenziali.



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Esempio-2: in questo esempio, un'e-mail in arrivo indica che le licenze Office 365 di un'organizzazione sono scadute. L'e-mail continua a dire all'utente di accedere a Office 365 Admin Center per controllare le informazioni di pagamento.



Tuttavia, esaminando attentamente l'indirizzo e-mail del mittente, si nota che tale indirizzo non esiste. In breve, è evidente che questa e-mail non è stata inviata da Office365.

5. Reti sociali

I siti di social network ci aiutano a condividere informazioni e a comunicare con gli altri. Purtroppo, questi siti rendono anche più facile per i cyber-attaccanti rintracciarvi e scoprire cosa state facendo. Proteggetevi proteggendo ogni account con una password forte e unica. Meglio ancora, usate una password diversa per ogni account e utilizzate l'autenticazione a due fattori, se disponibile. Molti siti di social network supportano anche applicazioni di terze parti. Installate solo le app di cui avete bisogno e solo da fonti affidabili. Controllate la valutazione, i commenti e le autorizzazioni di ogni app prima di installarla. Se un'app non vi serve più, disinstallatela o disabilitate il suo accesso al vostro profilo di social network.

Proprio come la posta elettronica e la messaggistica, i cyber-attaccanti possono tentare di

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

truffarvi sui siti di social network. Può inviare messaggi fingendo di essere un vostro amico. Se ricevete un messaggio strano o sospetto da un amico, contattatelo via e-mail o telefono, non rispondendo al messaggio. Infine, per proteggere la nostra Istituzione, non pubblicate informazioni riservate sulla nostra Istituzione su nessun sito web. Se avete domande su ciò che potete pubblicare o condividere sul lavoro, chiedete al vostro supervisore.

Dopo aver abilitato l'autenticazione a due fattori (verifica), un codice di sicurezza verrà inviato al telefono o all'app di autenticazione ogni volta che si accede al proprio account da un nuovo dispositivo o browser. È necessario inserire questo codice per poter effettuare l'accesso. Se un criminale informatico cerca di accedere al vostro account, non può farlo se non ha accesso al vostro telefono cellulare. Potrete anche accorgervi di un tentativo di accesso al vostro account perché riceverete una notifica con un codice. Non condividete mai questo codice con altri! Un malintenzionato cercherà di appropriarsene. Se avete ricevuto il codice ma non avete provato ad accedere, cancellate il messaggio di codice e cambiate la password il prima possibile.

Esercizi 4:

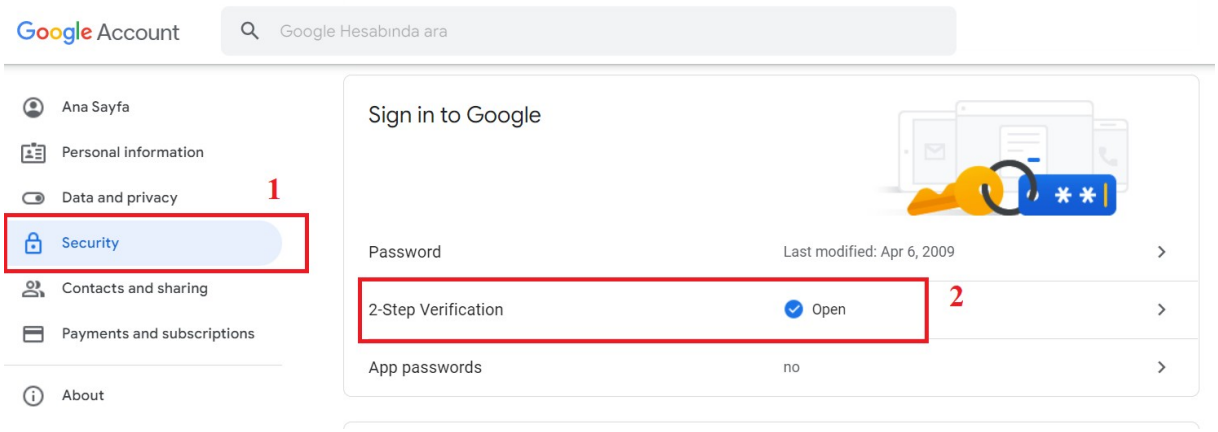
Eseguire l'autenticazione a due fattori - verifica per accedere all'account e-mail creato. Il primo di questi processi è la password che si utilizza per accedere all'account. L'altro può essere un codice di verifica (SMS) da inviare al telefono o un link di conferma da inviare a un altro indirizzo e-mail.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

La schermata seguente mostra come attivare la funzione di autenticazione a due fattori dell'account Gmail.
Completate la procedura e provate ad accedere nuovamente al vostro account e-mail.

Fase 1: aprire l'account Google.
Fase 2: Fare clic sulla sezione "Impostazioni".
Fase 3: selezionare la scheda "Sicurezza" dal menu sul lato sinistro della pagina che si apre (1). Attivare quindi la funzione "Verifica in due passaggi" al centro della pagina.



1.7. Le migliori pratiche per politiche di sicurezza informatica di successo

1. **Classificazione delle informazioni e dei dati:** Può rendere il vostro programma di sicurezza un successo o un fallimento. Una scarsa classificazione delle informazioni e dei dati può lasciare i sistemi aperti agli attacchi. Inoltre, una gestione inefficiente delle risorse può comportare spese generali. Una chiara policy di classificazione aiuta le organizzazioni a controllare la distribuzione delle risorse di sicurezza.
2. **Operazioni e amministrazione IT:** devono collaborare per soddisfare i requisiti di conformità e sicurezza. La mancanza di cooperazione tra i reparti può portare a errori di configurazione. I team che lavorano insieme possono coordinare la valutazione e l'identificazione dei rischi attraverso tutti i reparti per ridurli.
3. **Piano di risposta agli incidenti di sicurezza:** Aiuta ad avviare le azioni di ripristino appropriate durante gli incidenti di sicurezza. Una strategia per gli incidenti di sicurezza fornisce una linea guida che include la risposta iniziale alle minacce, l'identificazione delle priorità e le soluzioni appropriate.
4. **Policy SaaS e cloud** - fornisce all'organizzazione linee guida chiare per l'adozione del cloud e del SaaS, che possono costituire la base per un ecosistema cloud unificato. Questa policy può contribuire a mitigare le complicazioni inefficaci e l'uso improprio

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

delle risorse cloud.

5. **Politiche di utilizzo accettabili (AUP):** Aiutano a prevenire le violazioni dei dati che si verificano a causa di un uso improprio delle risorse aziendali. Le AUP trasparenti aiutano a mantenere tutto il personale in linea con l'uso corretto delle risorse tecnologiche aziendali.
6. **Policy di accesso e gestione delle identità (IAM):** Definisce come gli amministratori IT autorizzano i sistemi e le applicazioni ai dipendenti giusti e come i dipendenti creano le password per rispettare gli standard di sicurezza. Una semplice policy sulle password può ridurre i rischi legati all'identità e all'accesso.
7. **Policy di sicurezza dei dati:** Delinea i requisiti tecnici e gli standard minimi accettabili per la sicurezza dei dati, al fine di rispettare le leggi e le normative pertinenti.
8. **Regolamenti sulla privacy**: Le normative governative, come il Regolamento generale sulla protezione dei dati (GDPR), proteggono la privacy degli utenti finali. Le organizzazioni che non proteggono la privacy dei propri utenti rischiano di perdere la propria autorità e di essere multate.
9. **Policy sui dispositivi personali e mobili:** Definisce se i dipendenti possono utilizzare dispositivi personali per accedere all'infrastruttura aziendale e come ridurre il rischio di esposizione delle risorse di proprietà dei dipendenti. Oggi la maggior parte delle organizzazioni è passata al cloud. Le aziende che incoraggiano i dipendenti ad accedere alle risorse software aziendali da qualsiasi luogo, rischiano di introdurre vulnerabilità attraverso dispositivi personali come laptop e smartphone. La creazione di una policy per la corretta sicurezza dei dispositivi personali può aiutare a prevenire l'esposizione alle minacce attraverso le risorse di proprietà dei dipendenti.
10. **Policy di accesso remoto**: Delinea i metodi accettabili di connessione remota alle reti interne.
11. **Policy sulla posta elettronica/comunicazione**: Delinea le modalità di utilizzo da parte dei dipendenti del canale di comunicazione elettronica scelto dall'azienda, come e-mail, Slack o social media.
12. **Policy di disaster recovery**: Delinea il contributo dei team di cybersecurity e IT dell'organizzazione a un piano generale di continuità operativa.
13. **Piano di continuità aziendale (BCP):** Coordina gli sforzi di tutta l'organizzazione e viene utilizzato in caso di disastro per ripristinare il funzionamento dell'azienda.
14. **Policy di risposta agli incidenti (IR)**: Un approccio organizzato al modo in cui l'organizzazione gestirà e porrà rimedio a un incidente.
15. **Policy di gestione delle modifiche**: Si riferisce al processo formale per apportare modifiche all'IT, allo sviluppo del software e alla sicurezza.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Domande

Domande di autovalutazione.

- Perché è importante una policy di sicurezza delle informazioni?
- Spiegare la policy di protezione delle password

Allegati *(presentazione PowerPoint, dispense, stampe, link, video…):*

Riferimenti:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html
https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.