ERASMEDIAH – RAFFORZAMENTO EDUCATIVO CONTRO L'IPERCONNETTIVITÀ DEI SOCIAL MEDIA NUMERO DI PROGETTO: 2023-1-HU01-KA220-YOU-000161173

# MODULO 5

# SICUREZZA INFORMATICA E SICUREZZA ONLINE

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.

Lezione 5.1

# Introduzione alle basi della sicurezza informatica

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.

Durata: 40 minuti

Lezione 5.1

# Introduzione alle basi della sicurezza informatica

**Obiettivi:**

- Sviluppare una chiara comprensione dei concetti fondamentali della sicurezza informatica, compresi termini chiave come minacce, vulnerabilità e rischi.
- Identificare le minacce online più diffuse, come phishing, malware, ransomware e attacchi di ingegneria sociale, e comprenderne l'impatto.
- Promuovere una mentalità proattiva nell'identificazione e nella risposta a potenziali incidenti di sicurezza informatica.

**Messaggio/i chiave:**

- Che tu sia un privato, una piccola impresa o un'azienda globale, comprendere le pratiche di base della sicurezza informatica è essenziale per proteggere la tua identità digitale.
- L'implementazione di semplici misure preventive può far risparmiare molto tempo, denaro e stress rispetto al ripristino successivo a un attacco informatico.

TIPO DI LEZIONE:

# Panoramica della lezione

Nel mondo digitale odierno, comprendere le basi della sicurezza informatica non è più un optional, ma una necessità. Questa lezione vi introdurrà ai principi fondamentali della sicurezza informatica, alle minacce più comuni e a soluzioni pratiche per migliorare la sicurezza online. Insieme, esploreremo come salvaguardare le risorse digitali personali e professionali, promuovendo una cultura di consapevolezza e resilienza informatica.

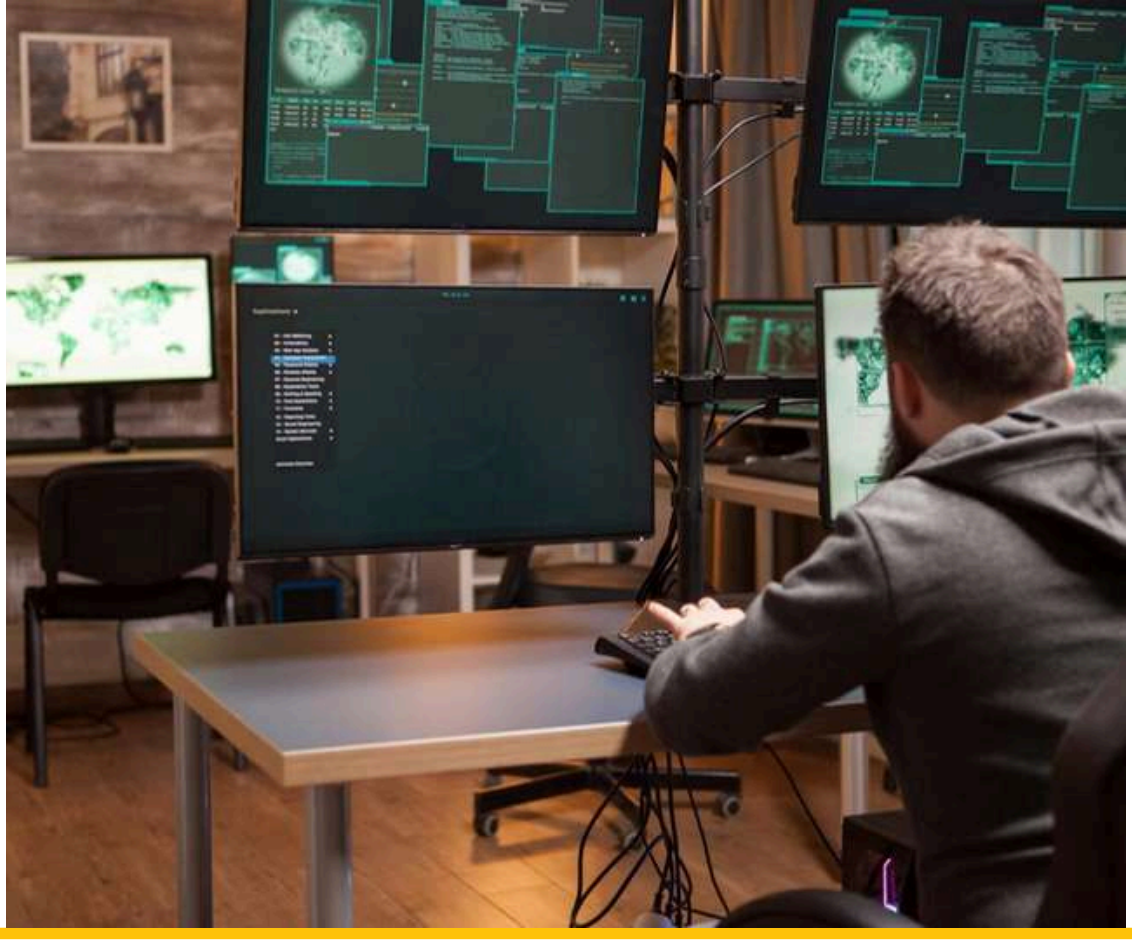
**Il workshop è organizzato in 4 fasi:**

1: Introduzione alle basi della sicurezza informatica (15 min)

2: Identificazione delle minacce informatiche più comuni (10 min)

3: Strategie per le migliori pratiche di sicurezza informatica (10 min)

4: Riflessione conclusiva e punti chiave (5 min)



Passo 1

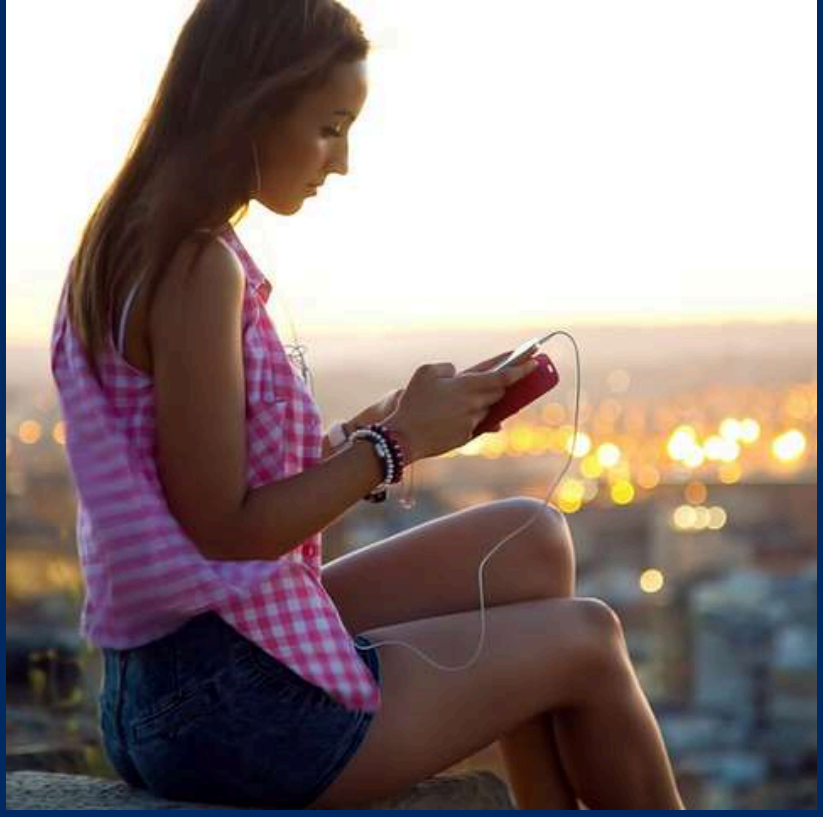
## Introduzione alle basi della sicurezza informatica

Iniziamo con un breve video che introduce il concetto di sicurezza informatica. Nella nostra vita quotidiana utilizziamo costantemente strumenti digitali, ma quanto spesso ci soffermiamo a considerare la loro sicurezza? La sicurezza informatica è essenziale per proteggere noi stessi e le nostre informazioni personali nel mondo digitale. Oggi approfondiremo le basi della sicurezza informatica e scopriremo perché è così importante.

**Guardiamo insieme questo video:**
https://youtu.be/inWWhr5tnEA?si=Pxp1YyvjrFdLoo38

Ora che abbiamo guardato il video, discutiamo:

1. Cosa vi ha colpito di più della sicurezza informatica nel video?
2. Perché ritieni che la sicurezza informatica sia importante nella nostra vita quotidiana?



Passo 1

## Introduzione alle basi della sicurezza informatica

La sicurezza informatica non riguarda solo la protezione dei sistemi, ma anche la comprensione dei nostri comportamenti online. Il modo in cui interagiamo con gli strumenti digitali può rafforzare la nostra sicurezza o renderci vulnerabili alle minacce.

Ora è il momento di prendervi un momento per riflettere sulla vostra vita digitale.

Scrivete le risposte alle seguenti domande:
Quanto spesso pensate alla sicurezza delle vostre attività online?
Riuscite a identificare abitudini che potrebbero mettere a rischio i vostri dati personali?
Preparatevi a condividere i vostri pensieri!


Passo 2

## Identificazione delle minacce informatiche più comuni

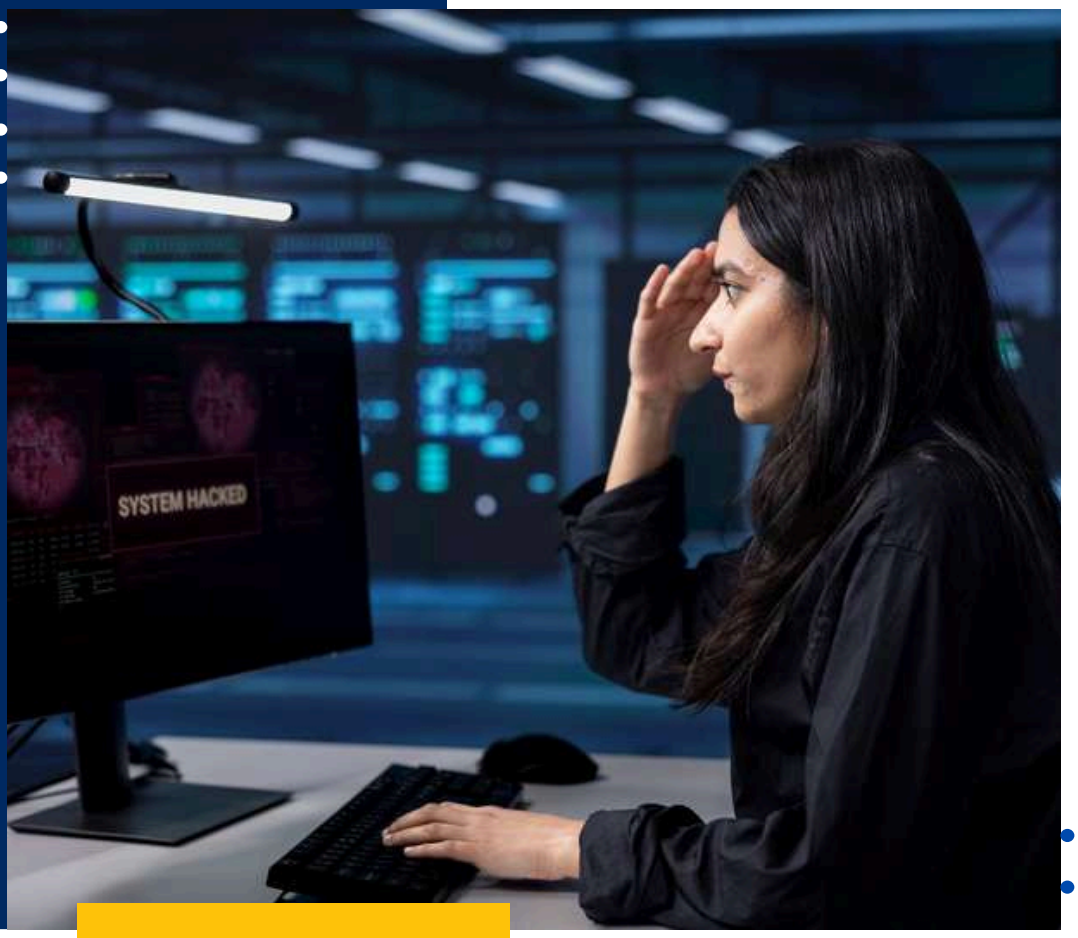
Diamo un'occhiata più da vicino ai tipi di minacce informatiche che potremmo incontrare.

Internet è un vasto spazio ricco di opportunità, ma presenta anche dei rischi. Le minacce informatiche possono colpire chiunque, ovunque, rendendo fondamentale comprenderne la natura e l'impatto. In questa fase, esploreremo i vari tipi di minacce e come possono influenzarci.

**Leggi l'articolo:** IBM: Tipi di minacce informatiche

L'articolo evidenzia:

- I diversi tipi di minacce informatiche, tra cui phishing, ransomware e malware.
- Come operano queste minacce e chi prendono di mira.
- Esempi dei danni che possono causare.




Passo 2

## Identificazione delle minacce informatiche più comuni

Dopo aver letto l'articolo, considerate quanto segue:

1. Quale tipo di minaccia informatica vi ha preoccupato di più e perché?
2. Voi o qualcuno che conoscete avete subito una di queste minacce?
3. Come pensate che comprendere queste minacce possa aiutare a prevenirle?

Dopodiché, scrivete un esempio o uno scenario reale (può essere ipotetico) in cui potrebbe verificarsi una delle minacce informatiche menzionate nell'articolo.

Preparatevi a condividere gli esempi e a discuterne nel  gruppo!

Passo 3

# Strategie per le migliori pratiche di sicurezza informatica

Ora concentriamoci sulla nostra protezione online.

Sebbene le minacce informatiche siano in continua evoluzione, ci sono misure semplici ed efficaci che possiamo adottare per salvaguardare le nostre informazioni e garantire la sicurezza. Adottando le migliori pratiche di sicurezza informatica, possiamo ridurre al minimo i rischi e rimanere più sicuri nella nostra vita digitale.

La sicurezza informatica non richiede competenze tecniche avanzate: piccole azioni intenzionali possono fare una grande differenza nella protezione di te stesso e dei tuoi dati.

Passo 3

# Strategie per le migliori pratiche di sicurezza informatica

Ecco alcune pratiche chiave da considerare:

- Creare password complesse e uniche e modificale regolarmente.
- Abilitare l'autenticazione a più fattori (MFA) per una maggiore sicurezza.
- Fare attenzione ai link e agli allegati, soprattutto se provenienti da fonti sconosciute.
- Mantenere aggiornati software e dispositivi per correggere le vulnerabilità.
- Utilizzare connessioni Wi-Fi sicure, evitando ove possibile le reti pubbliche.

**Attività:** Checklist delle migliori pratiche di sicurezza informatica

Fase 1: Valuta le tue abitudini attuali

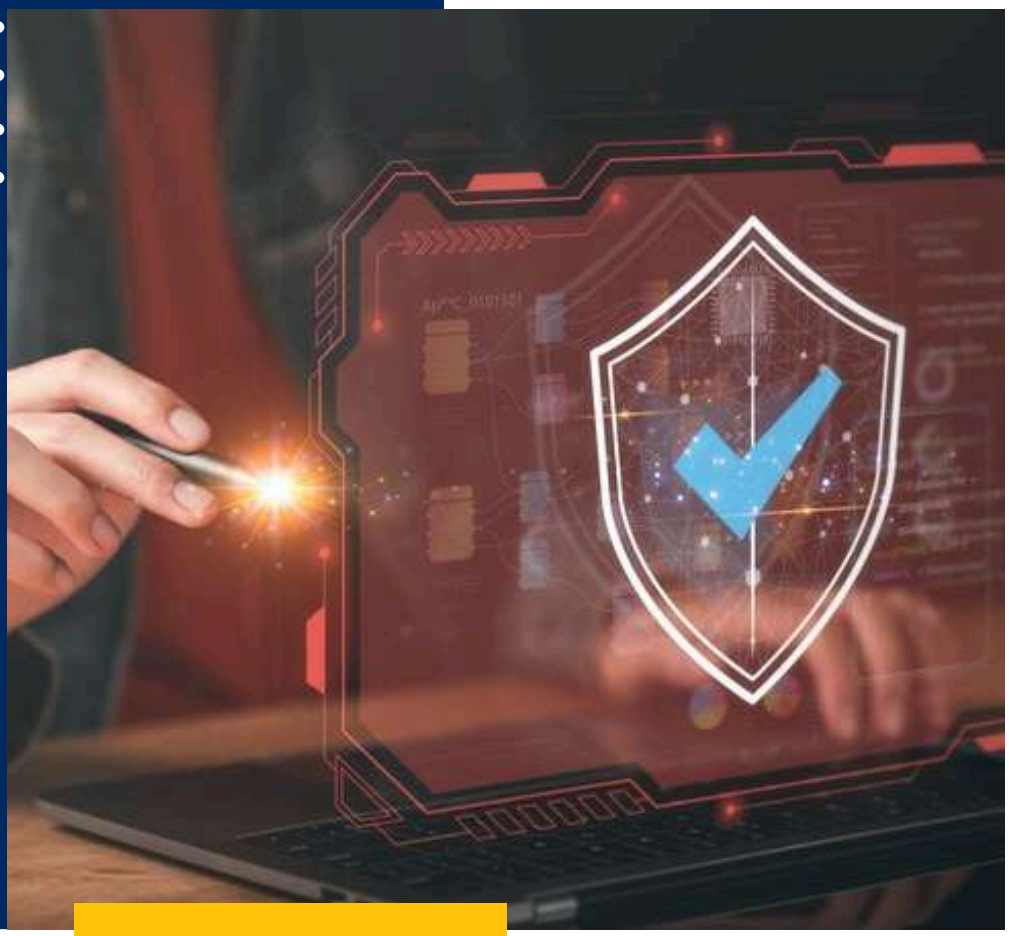
- Rifletti sui tuoi attuali comportamenti e abitudini online. Ci sono aree in cui potresti metterti a rischio?

Esempio: "Uso la stessa password su più account"

Fase 2: Creare un piano

- Scrivi un passaggio attuabile per ogni concetto chiave elencato sopra. Ad esempio:

Password complesse: "Installerò un gestore di password per generare e memorizzare password sicure", ecc.



Passo 3

# Strategie per le migliori pratiche di sicurezza informatica

Fase 3: condivisione di gruppo

- Condividi una delle azioni che hai pianificato con un partner o con il gruppo.
- Discuti di come questi passaggi potrebbero aiutarti a migliorare la tua sicurezza digitale.
- Offrire suggerimenti o consigli su ulteriori misure che altri possono adottare.

Alla fine, rispondi mentalmente e con attenzione **alla domanda chiave**:

Quale abitudine o strategia puoi iniziare a mettere in pratica oggi stesso per migliorare immediatamente la tua sicurezza online?

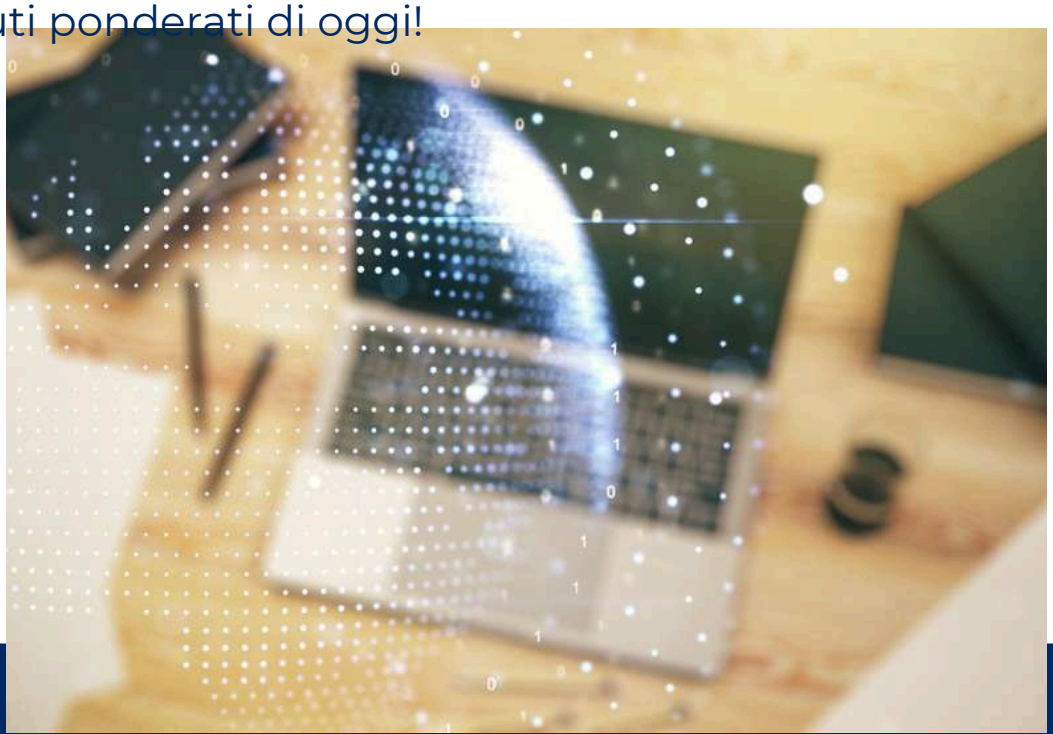
Passo 4

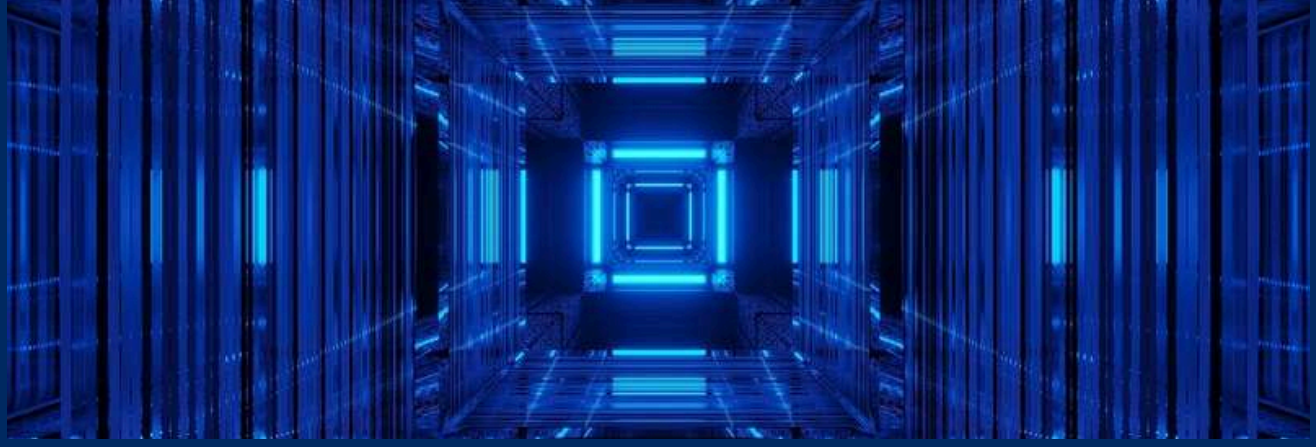
# Riflessione conclusiva e punti chiave

Per concludere, prendiamoci un momento per riflettere su tutto ciò che abbiamo trattato in questa lezione e su come possiamo usare queste conoscenze in futuro.

Pensate alle vostre abitudini online: ci sono cambiamenti che vi sentite ispirati a fare dopo la discussione di oggi? In tal caso, qual è il primo passo che fareste per migliorare la vostra sicurezza informatica?
Ora pensate a come possiamo aiutare gli altri. Qual è un semplice consiglio o un'abitudine emersa da questo workshop che potreste condividere con un amico o un collega per aiutarlo a rimanere al sicuro online?

Grazie a tutti per la vostra partecipazione attiva e per i vostri contributi ponderati di oggi!





## Riepilogo dei punti chiave

- **La sicurezza informatica è per tutti. Comprendere le minacce e adottare le migliori pratiche ci aiuta a rimanere al sicuro online.**
- **Piccoli passi fanno una grande differenza. Strumenti come i gestori di password e gli aggiornamenti regolari possono migliorare significativamente la tua sicurezza.**
- **Tenersi informati. Le minacce informatiche sono in continua evoluzione, quindi è fondamentale rimanere aggiornati sui suggerimenti e sugli strumenti più recenti per una sicurezza a lungo termine.**
- **Essere proattivi. Più si adott abitudini sicure, più si è al sicuro.**

# Istruzioni per operatori giovanili, educatori e insegnanti

**Obiettivo:**
Questa lezione si propone di aiutare operatori socio-educativi, educatori e insegnanti a fornire ai giovani le conoscenze essenziali sulla sicurezza informatica. Attraverso discussioni, attività e riflessioni coinvolgenti, i partecipanti comprenderanno le minacce informatiche più comuni, apprenderanno le migliori pratiche per la sicurezza online e creeranno piani attuabili per proteggersi nel mondo digitale.

**Materiali necessari:**

- Connessione Internet per la riproduzione di video o articoli
- Proiettore e schermo
- Altoparlanti
- Accesso agli strumenti di sicurezza informatica consigliati
- Carta da grafico o pennarelli per lavagna bianca
- Penne o matite
- Fogli di carta

**Fase 1: Introduzione alle basi della sicurezza informatica (15 min)**

1. Inizia coinvolgendo i partecipanti con un esempio pertinente: "Pensa all'ultima volta che hai utilizzato una nuova app o visitato un sito web. Ti sei mai fermato a pensare a quanto siano sicuri i tuoi dati?"

2. Evidenzia l'importanza della sicurezza informatica: spiega che la sicurezza informatica non è riservata solo ai professionisti IT; è una competenza fondamentale per tutti nell'era digitale odierna. Sottolineare come la sicurezza informatica contribuisca a proteggere le informazioni personali, professionali e aziendali.

3. Delineare chiaramente gli obiettivi della sessione.

4. Attività: Proiezione video e discussione:
- Guarda il video: "Cos'è la sicurezza informatica?" (guardalo qui).
- Dopo la visione, porre ai partecipanti delle domande guida.

5. Dopo il video, avvia una discussione:
- "Cosa ti ha sorpreso di più della sicurezza informatica?"
- "Pensi che la sicurezza informatica sia importante per tutti? Perché sì o perché no?"
- “Quali sono i rischi derivanti dalla mancata attenzione alla sicurezza online?”

**Fase 1: Introduzione alle basi della sicurezza informatica (15 min)**

6. Riflessione personale: chiedi ai partecipanti di prendersi qualche minuto per scrivere i propri pensieri:

- “Quanto spesso consideri la sicurezza delle tue attività online?”
- “Sai individuare una o due abitudini che potrebbero mettere a rischio le tue informazioni personali?”
- "Quali cambiamenti pensi di poter apportare per migliorare la tua sicurezza online?"

7. Incoraggiare la condivisione in coppia o in piccoli gruppi:

- Opzione 1: Condividi un'abitudine che ritieni rischiosa e chiedi consiglio al tuo gruppo su come migliorarla.
- Opzione 2: Discuti se hai mai subito o sentito parlare di una minaccia informatica e come è stata gestita.

8. Se i partecipanti preferiscono non condividere in gruppo, consenti loro di scrivere una modifica che si impegnano a fare e di inviarla in forma anonima al facilitatore per una discussione successiva.

**Fase 2: Identificazione delle minacce informatiche più comuni (10 min)**

1. Condividi l'articolo IBM: Tipi di minacce informatiche o un riepilogo stampato dei suoi punti chiave.
2. Assegna ai partecipanti 5 minuti per leggere e annotare le minacce che ritengono più preoccupanti, concentrandosi sul loro funzionamento e sul loro potenziale impatto.
3. Discussione:

Facilitare una conversazione di gruppo:

- “Quale minaccia informatica ritieni più preoccupante e perché?”
- "Tu o qualcuno che conosci ha mai subito una di queste minacce? Cosa è successo?"

4. integra con approfondimenti se necessario:

Evidenzia statistiche o esempi per arricchire la discussione, come e-mail di phishing o attacchi ransomware.

5. Attività di scenario:

Chiedi ai partecipanti di scrivere un breve esempio, reale o ipotetico, che riguardi una minaccia informatica, come ad esempio:

- Phishing: "Un'e-mail fraudolenta ha indotto qualcuno a condividere le credenziali di accesso del proprio account"
- Malware: "Cliccando su un link sospetto si scarica un virus, bloccando i file"

6. Condividere gli scenari nel gruppo e facilitare una discussione su:

- "Cosa è andato storto nello scenario?"
- “Come si sarebbe potuta evitare questa situazione?”
- “Quali misure preventive sarebbero state d’aiuto?”

7. Se riti, puoi contribuire alla discussione evidenziando strategie preventive concrete per ogni tipo di minaccia.

**Fase 3: Strategie per le migliori pratiche di sicurezza informatica (10 min)**

1. Panoramica delle migliori pratiche:
    - Presenta strategie semplici ed efficaci:
    - Utilizza password complesse e univoche.
    - Abilita l'autenticazione a più fattori (MFA).
    - Evita link e allegati sospetti.
    - Mantenere aggiornati software e dispositivi.
    - Utilizza una rete Wi-Fi sicura o una VPN.
- Utilizzare esempi concreti o brevi dimostrazioni per mostrare l'impatto di ciascuna strategia.

2. Se possibile, dimostra o spiega la configurazione di uno strumento (incluso nella sezione "Strumenti") per renderlo comprensibile.
3. Attività: checklist per la sicurezza informatica:

- Distribuisci un semplice modello di checklist con le strategie elencate.
- Chiedete ai partecipanti di scrivere un passaggio attuabile per ciascuno.
- Esempio: "Abiliterò l'MFA sulla mia email".
- Incoraggiate i partecipanti a concentrarsi su azioni semplici e immediate e, se necessario, aiutateli a chiarire i passaggi.

4. Condivisione di gruppo:

- I partecipanti condividono un passo che intendono compiere.
- Fornire un feedback rapido e incoraggiare la discussione sui vantaggi di questi cambiamenti.
- Incoraggiate i partecipanti a rivedere regolarmente la loro lista di controllo per aggiornare le loro abitudini.

**Fase 4 Riflessione conclusiva e punti chiave (5 min)**

1. Rafforzare l'apprendimento e motivare i partecipanti ad applicare ciò che hanno imparato.
2. Chiedere ai partecipanti:
   - "Qual è un'abitudine che intendi cambiare o adottare a partire da oggi?"
   - "Come condividerai con gli altri ciò che hai imparato?"
3. Condivisione di gruppo:
   - Invita i volontari a condividere le loro riflessioni o un messaggio importante.
4. Messaggio di chiusura:
   - Ricorda ai partecipanti: "La sicurezza informatica è responsabilità di tutti. Piccoli passi intenzionali possono fare una grande differenza nella sicurezza online".
   - Ringraziamo tutti per la loro partecipazione attiva e incoraggiamoli ad agire immediatamente.

**Punti chiave:**

Sottolineare ai partecipanti che la sicurezza informatica è una competenza necessaria a tutti, indipendentemente dalle proprie competenze tecniche. Utilizza i punti chiave della lezione per evidenziare come la comprensione delle minacce comuni e l'adozione di misure preventive, come l'utilizzo di password complesse o l'abilitazione dell'MFA, possano ridurre drasticamente i rischi online. Incoraggiare i partecipanti ad adottare una mentalità proattiva, definendo obiettivi semplici e raggiungibili per migliorare le proprie abitudini online. Rafforzare questi concetti attraverso discussioni di follow-up o attività che li riprendano, assicurandosi che i partecipanti rimangano vigili e motivati a mantenere solide pratiche di sicurezza informatica.

**Attività di follow-up e da svolgere a casa**

Incoraggiate i partecipanti a mettere in pratica quanto appreso monitorando le loro attività online nel corso della prossima settimana. Potranno identificare le aree in cui si sentono più vulnerabili e implementare una nuova strategia di sicurezza informatica ogni giorno. Inoltre, suggerite loro di provare a casa strumenti come LastPass o Bitdefender e di condividere le loro esperienze con il gruppo in una sessione di follow-up.

**Suggerimenti per gli insegnanti:**

Integrate i temi della sicurezza informatica nelle conversazioni o nelle lezioni quotidiane utilizzando esempi concreti che si riferiscono alle esperienze degli studenti, come la sicurezza dei social media o le truffe più comuni. Utilizzate metodi interattivi come discussioni di gruppo o scenari di gioco di ruolo per rendere l'argomento coinvolgente e pratico. Verificate regolarmente i progressi e offrite supporto per rafforzare l'importanza di costruire solide abitudini di sicurezza informatica.

# Strumenti

## LastPass

LastPass è un potente strumento di gestione delle password progettato per migliorare la sicurezza informatica generando e archiviando in modo sicuro password complesse e uniche per tutti gli account online. Elimina la necessità di ricordare più password complesse, archiviandole in un archivio digitale crittografato, accessibile solo con una password principale.

**www.lastpass.com**

## Bitdefender

Bitdefender è uno strumento di sicurezza informatica avanzato che offre una protezione completa contro malware, phishing, ransomware e altre minacce online. Combina un software antivirus affidabile con misure anti-phishing intelligenti per fornire una sicurezza multilivello per uso personale e professionale.

**www.bitdefender.com**

# Riferimenti


- Bitdefender. (n.d.). Recuperato da https://www.bitdefender.com
- Cisco Networking Academy. (n.d.). Nozioni fondamentali sulla sicurezza informatica. Cisco Networking Academy: impara la sicurezza informatica, Python e altro ancora. Tratto da https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US
- IBM. (25 marzo 2024). Tipi di minacce informatiche. Tratto da https://www.ibm.com/think/topics/cyberthreats-types
- Lakhwani, S. (19 giugno 2024). Fondamenti di sicurezza informatica [Guida per principianti 2024]. Blog di upGrad KnowledgeHut. Tratto da https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- LastPass. (n.d.). Recuperato da https://www.lastpass.com
- Simplilearn. (10 giugno 2020). Cos'è la sicurezza informatica | Come funziona? | Sicurezza informatica in 7 minuti | Sicurezza informatica | Simplilearn. [Video]. YouTube. https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo

# QUIZ

1. Qual è uno degli obiettivi principali della sicurezza informatica?
A. Garantire che nessuno possa accedere a Internet senza autorizzazione
B. Consentire alle aziende di monitorare l'attività degli utenti
C. Proteggere le risorse digitali gestendo rischi e vulnerabilità
D. Bloccare tutte le e-mail provenienti da mittenti sconosciuti

2. Quale delle seguenti affermazioni dimostra l'utilizzo dell'autenticazione a più fattori (MFA)?
A. Effettuando l'accesso rispondendo a una domanda di sicurezza
B. Utilizzando la password della tua e-mail e un'e-mail di backup per il recupero
C. Combinando una password con un codice temporaneo inviato al tuo telefono
D. Salvando le password in un file crittografato sul tuo computer

3. Cosa distingue il phishing dalle altre minacce online?
A. Implica l'hacking diretto dei sistemi senza l'interazione dell'utente.
B. Utilizza tattiche ingannevoli per indurre gli utenti a condividere informazioni sensibili.
C. Si diffonde attraverso dispositivi fisici come le unità USB.
D. Funziona esclusivamente installando malware su un computer.

# QUIZ

4. In che modo l'aggiornamento del software migliora la sicurezza informatica?
A. Migliora la progettazione e l'usabilità delle tue applicazioni
B. Riduce le possibilità che i bug interferiscano con le tue attività
C. Chiude le falle di sicurezza che gli aggressori potrebbero sfruttare
D. Consente una migliore compatibilità con hardware più vecchio

5. Perché è utile utilizzare un gestore di password?
A. Garantisce che tutte le tue password vengano sottoposte a backup su un server condiviso
B. Disconnette automaticamente dagli account dopo un periodo di tempo impostato
C. Crea e memorizza in modo sicuro password complesse per ogni account
D. Avvisa quando qualcuno accede alla tua posta elettronica senza autorizzazione

# Soluzioni

Domanda 1: C
Domanda 2: A
Domanda 3: B
Domanda 4: B
Domanda 5: A

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

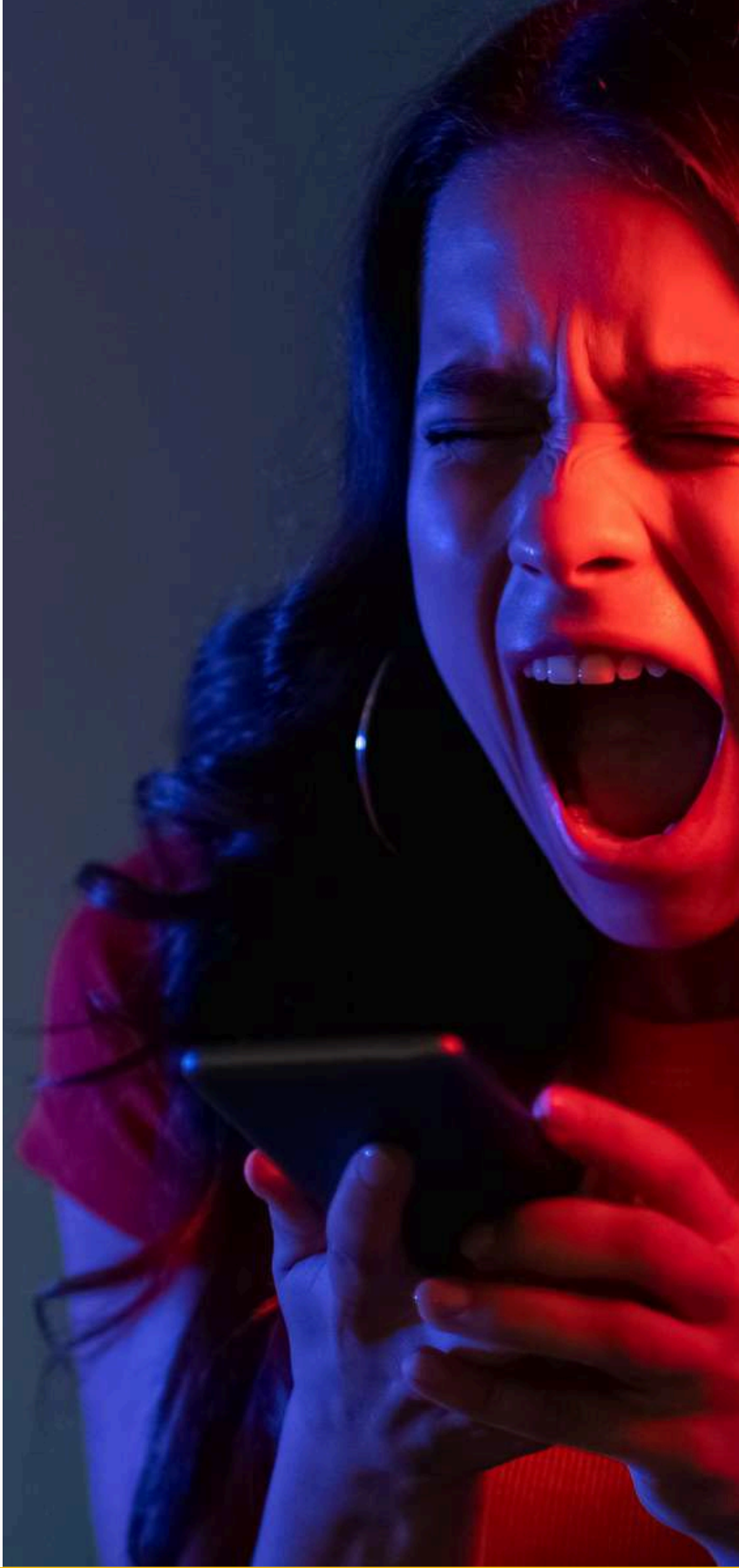
LABC

Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.