Scheda di formazione

Titolo	Sicurezza informatica: strumenti per una navigazione sicura
Parole chiave	Cyber security, sicurezza online, dipendenza digitale, navigazione sicura, tecnologia sanitaria
Fornito da	Croatian Telecom Inc.
Lingua	Italiano

Area di formazione (X se applicabile)	
	Alfabetizzazione all'informazione
	Comunicazione e collaborazione
x	Sicurezza
	Problem Solving

Obiettivi / Risultati dell'apprendimento

Obiettivo: L'obiettivo di questa formazione è quello di educare gli anziani alla sicurezza informatica e di fornire loro gli strumenti e le conoscenze necessarie per navigare in modo sicuro nel mondo online.
Risultati dell'apprendimento: al termine di questa formazione, i partecipanti saranno in grado di:

- Comprendere l'importanza della sicurezza informatica
- Riconoscere le minacce informatiche più comuni
- Praticare una navigazione sicura in Internet
- Salvaguardare le informazioni personali
- Rispondere agli incidenti informatici
- Identificare i rischi delle tecnologie digitali per la salute e il benessere
- Utilizzare le tecnologie digitali per la salute e il benessere

Descrizione

Questa formazione fornisce agli anziani le conoscenze e gli strumenti essenziali per navigare in sicurezza nel mondo online. I partecipanti impareranno a conoscere i rischi della sicurezza informatica e a riconoscere le minacce più comuni. Comprenderanno la navigazione sicura in Internet e la sicurezza della posta elettronica, la protezione dei dispositivi personali, la salvaguardia delle informazioni personali e la sicurezza. Il corso copre anche la risposta agli incidenti e l'importanza di tenersi aggiornati sulle minacce informatiche emergenti. Saranno inoltre in grado di navigare in modo sicuro nelle tecnologie digitali in relazione alla loro salute e al loro benessere, prendendo decisioni informate e sfruttando le opportunità che offrono. Alla fine, si sarà in grado di proteggere sé stessi e le proprie informazioni personali online.

Indice di contenuto (3 livelli)

Modulo: Sicurezza informatica: strumenti per una navigazione sicura

Co-funded by the European Union

Unità 1: Introduzione alla sicurezza informatica
1.1. Comprendere i rischi della sicurezza informatica
1.2. Tipi comuni di minacce informatiche
1.3. Importanza della sicurezza informatica per gli anziani

Unità 2: Navigazione sicura in Internet
2.1. Le migliori pratiche per mantenersi al sicuro nell'ambiente digitale
2.2. Migliorare la sicurezza online con strumenti di navigazione sicuri

Unità 3: Salute e benessere nell'era digitale
3.1. Rischi dell'eccessivo tempo trascorso sullo schermo e della dipendenza digitale
3.2. Salute e strumenti digitali

Contenuto sviluppato

Modulo: Sicurezza informatica: strumenti per una navigazione sicura

Unità 1: Introduzione alla sicurezza informatica
Sezione1.1.: Comprendere i rischi della sicurezza informatica
Considerare i rischi della sicurezza informatica come potenziali pericoli quando si va online. Proprio come si prendono precauzioni per stare al sicuro nel mondo fisico, come chiudere a chiave le porte, essere consapevoli dei rischi informatici aiuta a stare al sicuro nel mondo digitale. Questi rischi possono essere rappresentati da hacker che cercano di rubare le vostre informazioni personali, da truffe che costringono a consegnare il proprio denaro o da virus che possono danneggiare il proprio computer. Inoltre, la sicurezza informatica enfatizza la coltivazione di una cultura consapevole della sicurezza, promuovendo la consapevolezza e l'educazione alle pratiche sicure online.
Imparando a conoscere questi rischi, è possibile proteggersi meglio. È come conoscere i segnali di un pavimento scivoloso per camminare con attenzione ed evitare di cadere. Si parlerà dei rischi informatici più comuni e di come riconoscerli, in modo che si possa navigare nel mondo online con fiducia e fare scelte informate per mantenere al sicuro se stessi e le proprie informazioni. Ricordare che la conoscenza è potere e che, comprendendo i rischi della sicurezza informatica, si farà un passo importante verso la protezione online.

1.2. Tipi comuni di minacce informatiche
In questa unità si esploreranno i tipi più comuni di minacce informatiche, ovvero i diversi modi in cui i malintenzionati cercano di danneggiare l'utente o il computer quando si utilizza Internet. La comprensione di queste minacce aiuta a stare al sicuro e a evitare potenziali danni. Vediamo di capire in termini semplici.
Considerare le minacce informatiche come trucchi o trappole subdole che i malintenzionati utilizzano online. Vogliono rubare le vostre informazioni personali, infettare il vostro computer con un software dannoso o ingannarvi per far sì che diate il vostro denaro. Alcuni tipi comuni di minacce informatiche sono il phishing, il malware e il furto di identità.

Co-funded by the European Union

Il phishing è un messaggio o un'e-mail fasulli che fingono di provenire da una persona fidata, ma che cercano di ingannare l'utente per indurlo a fornire le sue informazioni personali. È come se qualcuno fingesse di essere un amico per avere accesso ai vostri segreti. I messaggi di phishing più comuni sono: false e-mail dalla banca, false segnalazioni di vincite al gioco d'azzardo o di premi gratuiti, falsi account di fornitori di servizi informatici o di pagamento o di negozi su Internet, false conferme di presunti ordini o falsi solleciti di pagamento, falsi messaggi sulle politiche di privacy dei dati personali o sulle condizioni da accettare.
Il messaggio e-mail di phishing può dire: La tua carta di credito è scaduta, il tuo account è scaduto, temporaneamente bloccato, o confermare i tuoi dati di accesso. Il layout (corporate design), l'indirizzo del mittente o il saluto diretto all'utente possono creare l'impressione che si tratti di un'e-mail inviata da una banca o da un altro servizio di provider. I messaggi e-mail in formato HTML mostrano al destinatario un link ‘‘legale’’, che contiene un link nascosto sullo sfondo, che conduce direttamente a contenuti fraudolenti o dannosi.
Il malware è come un virus che può infettare il computer e causare danni. Può rallentare il computer o addirittura rubare le informazioni personali. Il furto di identità avviene quando qualcuno ruba le vostre informazioni personali, come il nome, l'indirizzo o i dati della carta di credito, e le utilizza senza il vostro permesso. È come se qualcuno fingesse di essere voi e utilizzasse il vostro denaro o acquistasse cose per vostro conto.
I ladri d'identità possono anche integrare nei loro messaggi di posta elettronica malware come virus software Trojan come link, allegato o codice sorgente in un messaggio e-mail in formato HTML. Basta cliccare sull'immagine del messaggio di phishing per avere gravi conseguenze. I truffatori che rubano le identità spesso utilizzano indirizzi che differiscono solo leggermente da quelli originali. Un ladro di identità può sostituire i caratteri per creare URL falsi. Ad esempio, al posto degli indirizzi originali, come http://www.onlinebank.com.hr, può essere utilizzata una rappresentazione fittizia di un indirizzo come http://www.on1inebank.com.hr.

Come sapere se qualcosa è dannoso?

- INDIRIZZO FALSO DEL MITTENTE

Passare il mouse sull'indirizzo del mittente. L'indirizzo e-mail contiene elementi sospetti? Ci sono errori di ortografia nell'indirizzo, anche se insignificanti?

- RICHIESTA DI DATI RISERVATI

Il link contenuto nell'e-mail chiede di inserire informazioni personali? Viene richiesto di fornire informazioni riservate come PIN o password?

- URGENZA

L'e-mail richiede di agire immediatamente o con urgenza? Il messaggio contiene una minaccia o un avvertimento?

- COLLEGAMENTI A SITI WEB FALSI

Quale URL appare quando si passa il mouse su un link? Si tratta di una pagina sicura (l'URL deve iniziare con "https://") e criptata (simbolo del lucchetto davanti all'URL)?

- COLLEGAMENTI A SITI WEB FALSI

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Il messaggio di posta elettronica è generico? Contiene errori di ortografia, punteggiatura errata o segni particolari? Imparando a conoscere questi tipi comuni di minacce informatiche, è possibile riconoscerli e adottare misure per proteggersi. Si discuteranno le strategie per rimanere al sicuro ed evitare di cadere vittima di queste minacce, consentendo di godere del mondo online con fiducia e tranquillità.

1.3. Importanza della sicurezza informatica per gli anziani

Pensare alla sicurezza informatica come alla propria guardia del corpo personale nel mondo digitale, che veglia sul vostro benessere. È come avere qualcuno che veglia su noi stessi, assicurandosi che le nostre informazioni personali siano al sicuro e che i nostri dispositivi siano protetti. Per garantire la sicurezza informatica, dobbiamo adottare abitudini online sicure, come creare password forti e uniche, essere cauti nel cliccare su link sospetti o scaricare file da fonti sconosciute e mantenere aggiornati i nostri dispositivi e software.

- Non confermare mai il numero di conto, la password o altre informazioni segrete se richieste in un messaggio di posta elettronica. Le banche e le aziende reali non lo farebbero mai per motivi di sicurezza.
- Controllare lo stato di sicurezza dei siti web prima di inserire i propri dati personali. L'HTTPS non garantisce che un sito web sia reale. Fare clic sul simbolo del lucchetto visualizzato accanto all'URL nel browser per verificare il certificato di sicurezza del sito.
- Credere nell'infallibilità della tecnologia può lasciare spazio agli attacchi di phishing. Un sano livello di sfiducia impedisce agli aggressori di rubare la vostra identità e di accedere ai vostri account e sistemi informatici.

Unità 2: Navigazione sicura in Internet

2.1. Le migliori pratiche per mantenersi al sicuro nell'ambiente digitale

- Praticare abitudini di navigazione sicure: Quando si fa shopping, operazioni bancarie o condivisione di informazioni personali online, rivolgersi a siti web affidabili. Cercare il simbolo del lucchetto e "https://" nell'indirizzo del sito web, che indica una connessione sicura.
- Diffidare dell'ingegneria sociale: Diffidare di chiamate, messaggi o e-mail non richieste che richiedono informazioni personali o dettagli finanziari. Le organizzazioni legittime non chiedono tali informazioni con mezzi non richiesti.
- Eseguire regolarmente il backup dei dati: Creare backup dei file e dei dati importanti su un dispositivo di archiviazione separato o su un servizio cloud. Questo aiuta a proteggere dalla perdita di dati dovuta a guasti hardware, furti o attacchi ransomware.
- Attivare l'autenticazione a due fattori (2FA): Attivare la 2FA ogni volta che è disponibile. Questo aggiunge un ulteriore livello di sicurezza richiedendo una seconda fase di verifica, come un codice unico inviato al dispositivo mobile, oltre alla password.

Co-funded by the European Union

- Attenzione alla condivisione sui social media: Fare attenzione quando si condividono informazioni personali, dettagli sulla posizione o piani di vacanza sulle piattaforme dei social media. Un'eccessiva condivisione può fornire informazioni preziose a criminali informatici o potenziali ladri.
- Proteggere i dispositivi mobili: Applicare funzioni di sicurezza, come codici di accesso, impronte digitali o riconoscimento facciale, per bloccare smartphone e tablet. Installare applicazioni di sicurezza affidabili che offrano funzioni come la localizzazione e la cancellazione a distanza in caso di smarrimento o furto.
- Fidarsi del proprio istinto: se qualcosa sembra troppo bello per essere vero o è sospetto, fidarsi del proprio istinto. Essere scettici di fronte a offerte inaspettate, richieste di denaro o appelli urgenti per ottenere informazioni personali.
- Cancellare regolarmente i dati di navigazione: Cancellare regolarmente la cronologia di navigazione, i cookie e i dati memorizzati nella cache. Questo aiuta a proteggere la propria privacy rimuovendo le informazioni memorizzate che potrebbero essere accessibili a persone non autorizzate.

2.2. Migliorare la sicurezza online con strumenti di navigazione sicuri

Migliorare la sicurezza online con strumenti di navigazione sicuri è un aspetto importante della sicurezza informatica. Utilizzando questi strumenti, si può proteggere la propria privacy, mettere al sicuro le informazioni personali e ridurre il rischio di minacce online. Ecco alcuni consigli essenziali per migliorare la propria sicurezza online con strumenti di navigazione sicuri:

- Installare e utilizzare un browser Web affidabile: Scegliere un browser web affidabile, come Google Chrome, Mozilla Firefox o Microsoft Edge. Questi browser danno priorità alla sicurezza e rilasciano regolarmente aggiornamenti per risolvere le vulnerabilità.
- Attivare le funzioni di sicurezza del browser: Familiarizzare con le funzioni di sicurezza offerte dal browser web. Attivare funzioni come il blocco dei pop-up, la modalità di navigazione sicura e le impostazioni sulla privacy per migliorare la propria sicurezza online.
- Attivare la protezione da phishing e malware: Attivare le funzioni integrate di protezione dal phishing e dal malware offerte dal browser web. Queste funzioni possono avvertire di siti web sospetti e impedire di visitare siti dannosi noti.
- Rimanere istruiti e aggiornarsi: Rimanere informati sulle ultime minacce online e sulle migliori pratiche per una navigazione sicura. Leggere regolarmente fonti affidabili, come siti web o blog di sicurezza informatica, per rimanere aggiornati sull'evoluzione del panorama della sicurezza online.

Unità 3: Salute e benessere nell'era digitale

3.1. Rischi dell'eccessivo tempo trascorso sullo schermo e della dipendenza digitale

Per ridurre i rischi dell'eccessivo tempo trascorso sullo schermo e della dipendenza digitale, ecco alcune strategie e pratiche da considerare:

- Stabilire limiti di tempo per lo schermo: Stabilire limiti di tempo specifici per l'utilizzo degli schermi, sia per le attività di svago che per quelle legate al lavoro.

Co-funded by the European Union

Questo aiuta a creare un sano equilibrio tra il tempo trascorso sullo schermo e le altre attività.

- Fare pause regolari: Incorporare pause regolari dagli schermi nella routine quotidiana. Alzarsi, fare stretching e dedicarsi ad attività fisiche o hobby che non coinvolgano i dispositivi digitali.
- Praticare la disintossicazione digitale: Dedicare periodi specifici, come i fine settimana o le sere, per disconnettersi completamente dai dispositivi digitali. Usare questo tempo per dedicarsi ad attività offline, trascorrere del tempo con i propri cari o dedicarsi a degli hobby.
- Praticare l'uso consapevole della tecnologia: prestare attenzione a come si utilizza la tecnologia e all'impatto che ha sul proprio benessere. Riflettere sulle proprie abitudini digitali, valutarne gli effetti sulla propria vita e fare scelte consapevoli per ridurre al minimo le conseguenze negative.
- Cercare sostegno e responsabilità: Condividere le proprie preoccupazioni con familiari fidati, amici o gruppi di sostegno. Stabilire una responsabilità reciproca per incoraggiare un uso responsabile della tecnologia e fornire sostegno nel mantenimento di abitudini sane.
- Stabilire dei limiti digitali: Definire confini chiari per l'uso della tecnologia, come ad esempio disattivare le notifiche in orari specifici, evitare lo schermo prima di andare a letto o stabilire linee guida per l'uso dei dispositivi durante i pasti in famiglia.

Ricordare che l'obiettivo è sviluppare un rapporto sano con la tecnologia e fare in modo che arricchisca la propria vita, anziché diventare una fonte di eccessiva dipendenza. Attuando queste strategie, è possibile ridurre i rischi associati all'uso eccessivo dello schermo e promuovere uno stile di vita più equilibrato e soddisfacente.

3.2. Salute e strumenti digitali

La tecnologia può offrire numerosi modi per sostenere e migliorare la propria salute. Ecco alcuni modi in cui la tecnologia può aiutare la propria salute:

- Accesso alle informazioni: Internet offre una grande quantità di informazioni sulla salute, consentendo di ricercare sintomi, condizioni, trattamenti e misure preventive. Siti web affidabili, app per la salute e comunità online possono consentire di prendere decisioni informate sulla propria salute.
- Monitoraggio della salute: I dispositivi indossabili, come i fitness tracker e gli smartwatch, possono monitorare vari aspetti della salute, tra cui la frequenza cardiaca, il ritmo del sonno, l'attività fisica e le calorie bruciate. Questi dispositivi possono fornire indicazioni preziose sul benessere generale e aiutare a monitorare i progressi verso gli obiettivi di salute.
- Teleassistenza e consulti a distanza: I servizi di teleassistenza consentono di consultare gli operatori sanitari a distanza tramite videochiamate o chat online. Questo comodo approccio consente di risparmiare tempo e può essere particolarmente utile per appuntamenti di follow-up, controlli di routine o consultazioni mediche non urgenti.

Co-funded by the European Union

- Gestione dei farmaci: Le applicazioni mobili e gli organizer intelligenti per le pillole possono aiutare a gestire i farmaci fornendo promemoria per l'assunzione delle pillole, tracciando i programmi dei farmaci e fornendo avvisi per le ricariche delle prescrizioni. Questa tecnologia può evitare di saltare le dosi e promuovere l'aderenza ai regimi farmacologici.
- Supporto per la salute mentale: Diverse app e piattaforme online per la salute mentale forniscono risorse per gestire stress, ansia e depressione. Questi strumenti possono includere meditazione guidata, esercizi di respirazione, monitoraggio dell'umore e sessioni di terapia condotte attraverso piattaforme digitali.
- Gestione delle cartelle cliniche: Le cartelle cliniche digitali e i portali per i pazienti consentono di accedere e gestire la propria storia clinica, i risultati degli esami e il calendario degli appuntamenti. Questo semplifica la comunicazione con gli operatori sanitari e garantisce la continuità delle cure.
- Supporto e motivazione: Le comunità online e le piattaforme di social media dedicate alla salute e al benessere possono fornire supporto, motivazione e incoraggiamento. Connettersi con persone che la pensano nello stesso modo e può favorire un senso di comunità e aiutare a mantenere la responsabilità dei propri obiettivi di salute.
- Tracciamento della salute e analisi dei dati: La tecnologia consente di monitorare e analizzare i dati sulla salute nel tempo, come la pressione sanguigna, i livelli di glucosio nel sangue o il peso. Monitorando le tendenze e gli schemi, è possibile identificare le aree di miglioramento e apportare le modifiche necessarie per ottimizzare la propria salute.

Ricordare che la tecnologia può essere uno strumento prezioso per sostenere la salute, ma è importante usarla con saggezza e insieme a una consulenza medica professionale. Rivolgersi sempre a professionisti del settore sanitario per ottenere diagnosi accurate, raccomandazioni di trattamento e indicazioni personalizzate.

5 Voci del glossario

La sicurezza informatica si riferisce alla pratica di proteggere i sistemi informatici, le reti e le informazioni digitali da accessi non autorizzati, furti e danni. Comporta l'implementazione di misure per prevenire le minacce informatiche, come hacking, violazioni di dati e attacchi malware. L'obiettivo della cybersecurity è garantire la riservatezza, l'integrità e la disponibilità delle risorse digitali, salvaguardando individui e organizzazioni da potenziali rischi e vulnerabilità nel mondo digitale interconnesso.

Per furto di identità si intende l'acquisizione e l'utilizzo fraudolento di informazioni personali, come il nome, il numero di previdenza sociale o i dati finanziari di una persona, senza il suo consenso. Si tratta di impersonare la vittima per svolgere varie attività illegali, tra cui frodi finanziarie, acquisti non autorizzati o altre forme di reati legati all'identità.

L'ingegneria sociale è una tecnica di manipolazione utilizzata dai criminali informatici per ingannare gli individui e sfruttare la loro fiducia e le loro emozioni. Implica una manipolazione psicologica piuttosto che metodi tecnici per indurre le persone a rivelare informazioni sensibili o a eseguire azioni che potrebbero compromettere la

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

loro sicurezza. Esempi di tecniche di ingegneria sociale sono le e-mail di phishing, le truffe telefoniche, il pretexting e l'impersonificazione. L'obiettivo dell'ingegneria sociale è manipolare il comportamento umano per ottenere un accesso non autorizzato a sistemi, reti o informazioni personali.

5 domande di autovalutazione a scelta multipla

1. **Nella sicurezza informatica, i rischi si riferiscono a:**

a) Pericoli potenziali quando si va online
b) Misure di sicurezza online
c) Precauzioni contro i pavimenti scivolosi
d) Pratiche online sicure
Opzione corretta: a

2. **Quali sono alcuni tipi comuni di minacce informatiche?**

a) Attacchi fisici ai computer
b) Trucchi o trappole usati dai malintenzionati online
c) Misure di sicurezza per gli acquisti online
d) Strategie per proteggere le informazioni personali
Opzione corretta: b

3. **Che cos'è l'ingegneria sociale?**

a) Tecnica utilizzata dai criminali informatici
b) Lo studio del comportamento umano
c) Uno strumento di navigazione sicura
d) Un tipo di virus informatico
Opzione corretta: a

4. **Come si può migliorare la sicurezza online con strumenti di navigazione sicuri?**

a) Usando browser web affidabili e attivando le funzioni di sicurezza
b) Aumentando il tempo trascorso sullo schermo e la dipendenza digitale
c) Condividendo le informazioni personali sui social media
d) Ignorando le e-mail di phising e gli avvisi di malware
Opzione corretta: a

5. **Quali sono le strategie per mitigare i rischi dell'eccessivo tempo trascorso sullo schermo?**

a) Stabilire limiti al tempo trascorso sullo schermo e fare pause regolari
b) Aumentare l'uso della tecnologia per migliorare la salute
c) Disconnettersi completamente dai dispositive digitali
d) Cercare supporto e responsabilità
Opzione corretta: a

Bibliografia e ulteriori riferimenti

- https://staysafeonline.org/
- https://www.consumer.ftc.gov/topics/online-security

Co-funded by the European Union

▪ https://www.cisa.gov/cybersecurity ▪ https://www.getsafeonline.org/ ▪ https://us.norton.com/internetsecurity ▪ https://www.staysmartonline.gov.au/ ▪ https://www.commonsense.org/education/digital-citizenship/privacy-and-security	
Materiale correlato	BOOMER_Cyber_security_HT
Link di riferimento	
Video in formato Powtoon	https://www.youtube.com/watch?v=lvLhhqDhZJY

Co-funded by the European Union