ACCENTURE SECURITY AWARENESS
Programma del Corso

PREMESSA

Nel mondo sempre più digitalizzato in cui viviamo, la sicurezza informatica è diventata una priorità cruciale per aziende, organizzazioni e individui. La protezione delle informazioni sensibili, la prevenzione degli attacchi informatici e la gestione delle minacce online sono competenze essenziali per chiunque desideri navigare nel panorama tecnologico con fiducia e sicurezza.

La ASL di Latina comunica l'avvio di un percorso formativo obbligatorio, della durata di 2 anni, sviluppato su una piattaforma di "e-learning" in collaborazione con Accenture Security, pensata specificatamente per il personale aziendale e progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per un approccio "a rilascio costante e graduale".

Si sottolinea che la frequenza del corso è obbligatoria per tutti i dipendenti aziendali, come indicato da Linee Guida Regionali.

STRUTTURAZIONE

Il Corso verrà sviluppato in 2 annualità e prevede la seguente strutturazione:

- N. 24 Moduli per 2 annualità (n. 12 per anno) suddivisi in pillole di circa 7 minuti corredate da test di valutazione del livello di apprendimento. Tali moduli verranno erogati con la frequenza di uno al mese.
- Erogazione di N. 24 Video per 2 annualità (n. 12 per anno) di Alta qualità su base mensile della durata di 5-8 minuti che analizzano casi di attacchi/frodi cyber.

MODALITÀ DI EROGAZIONE

Il Corso verrà erogato in modalità e-learning mediante l'utilizzo delle seguenti piattaforme:

- Piattaforma Accenture Awareness per l'erogazione dei moduli formativi
- Piattaforma Accenture CHANNEL che permetterà la fruizione di video con riflessioni sul caso presentato

I ANNUALITÀ

MODULI AWARENESS EXPRESS	
PHISHING	Il PHISHING è la più comune tecnica di attacco utilizzata dai criminali Cyber e utilizza la mail come principale veicolo di diffusione, anche se si va estendendo velocemente ad altri canali, come i più popolari canali di messaggistica e i canali social. È particolarmente subdola perché basata su un inganno, con cui si cerca di indurre la potenziale vittima a compiere un'azione che consente al criminale di sferrare il suo attacco. Questo modulo formativo fornisce gli elementi cognitivi per riconoscere un attacco PHISHING e per adottare le necessarie contromisure.
PASSWORD	Uno dei pilastri della Cyber Security è rappresentato dalla PASSWORD, la chiave di accesso a tutte quelle risorse informatiche a cui si deve garantire un accesso

	sicuro e riservato. La gestione delle proprie PASSWORD diventa quindi un elemento basilare delle strategie difensive, della persona e dell'organizzazione. Questo modulo formativo fornisce gli elementi cognitivi necessari ad una gestione sicura delle PASSWORD, mettendole al riparo da tentativi di violazione che potrebbero avere conseguenze disastrose.
SOCIAL MEDIA	I SOCIAL MEDIA rappresentano una nuova modalità di socializzazione basata sulle ampie possibilità che la tecnologia digitale mette oggi a disposizione. Ma allo stesso tempo sono anche fattori di rischio, dove si può arrivare a compromettere sia la privacy delle persone sia la sicurezza dei sistemi delle organizzazioni. Questo modulo fornisce gli elementi cognitivi per utilizzare in modo consapevole questi strumenti, proteggendo la persona e l'organizzazione dai rischi che la condivisione in rete di contenuti individuali e professionali può generare.
PRIVACY & GDPR	L'introduzione del nuovo regolamento europeo sulla protezione dei dati aumenta la sensibilità delle organizzazioni rispetto alla PRIVACY e alla protezione dei dati sensibili. Al di là dei ruoli specifici, è importante che tutti i membri di un'organizzazione acquisiscano maggiore sensibilità rispetto alla protezione dei dati. Questo modulo fornisce gli elementi cognitivi per assumere un atteggiamento proattivo rispetto alla protezione dei dati, e per contribuire alla conformità dell'organizzazione rispetto alle nuove norme europee.
MOBILE & APP	I DEVICE MOBILI, soprattutto Smartphone e Tablet, sono strumenti che diventano ogni giorno più critici e che rappresentano la massima espressione della rischiosa sovrapposizione tra dimensione personale e professionale. Questo modulo fornisce gli elementi cognitivi per utilizzare i dispositivi mobili, siano essi personali o professionali, in modo consapevole, abilitando buone pratiche che siano in grado di aumentare il livello di sicurezza e di protezione dei dati.
FAKE NEWS	Le FAKE NEWS sono articoli redatti con informazioni inventate o semplicemente distorte, che hanno lo scopo di disinformare. Sono un fenomeno pericoloso, che se non controllato può avere ripercussioni negative sia per l'individuo sia per le organizzazioni. L'argomento viene spesso trattato dal punto di vista sociale e politico, ma ha anche una implicazione diretta con la Cyber Security. Questo modulo formativo fornisce gli elementi cognitivi necessari a riconoscere una Fake News, attivando alcuni processi di indagine che aiutano a sviluppare un atteggiamento corretto su qualsiasi informazione acquisita in rete.
USB DEVICE	Tutti i dispositivi USB, e in particolare i dispositivi di memorizzazione, possono diventare un punto critico rispetto alla necessità di proteggere le informazioni riservate, ed è per questa ragione che sono spesso oggetto di specifiche policy. Questo modulo formativo fornisce gli elementi cognitivi per riconosce tutti i rischi associati ai dispositivi USB, con particolare riferimento ai dispositivi di memorizzazione, abilitando buone pratiche per evitare di incorrere in fenomeni di sottrazione di dati.
EMAIL SECURITY	La MAIL è uno strumento sempre più importante, che nella vita professionale assume un ruolo centrale e particolarmente critico. Attraverso le MAIL vengono scambiate informazioni sensibili e quindi l'aspetto della sicurezza non può essere sottovalutato. Questo modulo formativo fornisce gli elementi cognitivi per le mail e le informazioni in esse contenute.
MALWARE & RANSOMWARE	I MALWARE in generale e il RANSOMWARE in particolare hanno conquistato velocemente gli onori della cronaca, mettendo in evidenza tutta la loro pericolosità. Le persone devono comprendere che i software antivirus non garantiscono la protezione totale rispetto a questi programmi maligni. Questo modulo formativo fornisce gli elementi cognitivi per ridurre il rischio di cadere vittima di questa particolare tipologia di software e per limitare le conseguenze negative in caso di violazione.
WEB BROWSING	La NAVIGAZIONE nel WEB presenta molti rischi e in quella che ormai sembra quasi un'attività scontata si presentano molti aspetti critici. Una buona conoscenza

	di alcune caratteristiche peculiari dei siti Web e dei browser può aiutare a ridurre notevolmente il livello di rischio. Questo modulo formativo fornisce gli elementi cognitivi su come navigare nel WEB in sicurezza.
CRITICAL SCENARIOS	Nell'interazione con il Cyber Spazio, esistono alcuni scenari critici: l'uso delle piattaforme Cloud, il viaggio di piacere o di affari, piuttosto che l'uso delle piattaforme di e-commerce, sia in ambito B2B che B2C. Sono scenari che risultano particolarmente esposti alla possibilità di subire attacchi da parte dei criminali Cyber, con rischi sia sul piano individuale sia sul piano professionale. Questo modulo vuole fornire elementi essenziali di consapevolezza che aiutano a comprendere le minacce, spesso sottovalutate, che sono collegate a questi particolari scenari di utilizzo delle tecnologie digitali.
SOCIAL ENGINEERING	Il social engineering, o ingegneria sociale, è la madre di tutte le strategie di attacco Cyber. È una strategia che punta sull'inganno e sulla manipolazione psicologica per perseguire finalità truffaldine. Per rendere più efficace l'attacco, il nucleo di questa strategia è costituito dall'acquisizione di informazioni sulla vittima designata. Questo modulo fornisce elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli precedenti.

VIDEO	
CEO Fraud	Dal paradiso all'inferno in un click. La truffa del CEO è una truffa online sempre più efficace e sempre più diffusa, che causa danni economici per chi la subisce. Il truffatore invita un dipendente a intraprendere un'azione, in risposta a una richiesta che apparentemente arriva da una persona senior della stessa organizzazione. L'azione consiste in un pagamento in contanti oppure nella comunicazione di informazioni sensibili, che però vanno a beneficio di un'organizzazione criminale. Non importa se non sei un CEO o una figura apicale della tua organizzazione: lo schema di attacco di questa truffa, può colpire chiunque in qualsiasi momento.
Smart Working	La tempesta perfetta. Sotto la spinta dell'emergenza legata alla pandemia da Covid19, la diffusione dello smart working, è stata rapida e, alcune volte, incontrollata. La pericolosa sovrapposizione tra dimensione privata e dimensione professionale rende la superficie di attacco molto più ampia e vulnerabile. L'ambiente casalingo e la distrazione possono essere complici inconsapevoli di un attacco cyber dai risvolti devastanti.
Password	È solo un gioco! La password è la chiave di accesso al nostro mondo digitale. Dareste mai le vostre chiavi di casa ad uno sconosciuto? L'attenzione alla password è un elemento fondamentale per la tutela della sicurezza delle nostre informazioni e della nostra identità in rete.
USB Device	Per un "pugno" di canzoni. Inserire una chiavetta USB in un computer è diventato un gesto quasi naturale. Ma dietro a quel dispositivo, all'apparenza innocuo, può nascondersi con facilità un pericolosissimo Malware. Questo fenomeno è accentuato dall'uso promiscuo di dispositivi personali e dispositivi aziendali, che amplia ancora di più la superficie di attacco a disposizione dei criminali Cyber.
Public Wi-Fi	Impigliata nella rete. Siamo ormai abituati ad essere costantemente interconnessi e ogni luogo pubblico mette a disposizione Wi-Fi liberi per i suoi visitatori. Dietro questa grande comodità può, tuttavia, nascondersi un rischio importante per la nostra sicurezza digitale. I Wi-Fi pubblici, soprattutto quelli "liberi", cioè non protetti da password, sono il mezzo ideale per le attività fraudolente, come furti di informazioni o diffusione di Malware.

SOCIAL ENGINEERING	Il peggiore affare di sempre. Gli attacchi di Social Engineering, basati sulla manipolazione psicologica della vittima, diventano sempre più pericolosi e sofisticati. Per prevenirli, dobbiamo alzare il livello di guardia rispetto al nostro modo di interagire con le tecnologie digitali, dando maggiore valore alla nostra privacy e valutando attentamente le possibili conseguenze delle nostre pubblicazioni in rete.
DEEPFAKE	Le vie dei truffatori sono infinite. Il Deepfake è la nuova frontiera degli attacchi Cyber, un vero e proprio salto di qualità nelle strategie criminali. Questa tecnica di falsificazione dei video, degli audio e delle immagini che fa ricorso all'Intelligenza Artificiale, deve renderci ancora più cauti di fronte a messaggi che ci inducono a fare delle azioni in situazioni anomale e impreviste.
RANSOMWARE	Impara a leggere! Ransomware: uno degli attacchi più pericolosi della dimensione Cyber, in grado di mettere in ginocchio qualsiasi organizzazione. Si tratta di un'emergenza planetaria, la vera pandemia della società digitale. Il miglior modo di affrontare un'infezione di questo tipo è ridurre il rischio di contrarla. Ricordate sempre: la prevenzione dipende solo da voi e dai vostri comportamenti.
SIM SWAP	L'insostenibile leggerezza del conto in banca. Chi avrebbe mai pensato che lo smartphone avrebbe assunto una funzione così critica, al punto da diventare un obiettivo della criminalità informatica? In questo episodio analizziamo una truffa particolarmente sofisticata, nota con il nome di SIM Swap, con cui un'organizzazione criminale può assumere il controllo della nostra utenza telefonica, con conseguenze molto gravi.
IDENTITY THEFT	In troppi vogliono essere nei vostri panni. Una minaccia sempre più diffusa è il cosiddetto furto di identità, che nella dimensione digitale può avvenire in molti modi. In questo episodio si riflette su questa minaccia, cercando di porre l'attenzione sull'importanza dei dati personali e sulle conseguenze che potrebbero derivare dall'uso improprio che criminali senza scrupoli potrebbero fare di questi dati.
SCAM WEBSITES	La tecnica del coccodrillo. Così come il coccodrillo attende le sue prede nascosto in una pozza d'acqua, così i criminali Cyber attendono le loro prede nascosti nella rete Internet. In questo episodio, si pone l'attenzione su una particolare truffa che riproduce, in formato digitale, la tecnica del coccodrillo, una tecnica che viene appunto etichettata con il termine di "watering hole".
SMISHING	Rimborso fatale. La nuova frontiera dell'inganno prende il nome di smishing: una declinazione della tecnica di attacco Cyber più diffusa, quella del phishing, ma realizzata tramite l'invio di sms ingannevoli o comunque attraverso l'uso di un sistema di messaggistica. In questo episodio si ricostruisce una truffa dalle conseguenze molto gravi, realizzata proprio con questa tecnica.

II ANNUALITÀ

MODULI AWARENESS EXPRESS	
CLEAN DESK	Mantenere una particolare attenzione verso la propria postazione di lavoro, evitando di lasciare informazioni critiche o addirittura sensibili nella disponibilità di persone non autorizzate ad accedervi, è un elemento basilare per garantire la sicurezza delle informazioni, la protezione dei dati, e quindi anche il rispetto delle normative sulla privacy. Questo modulo oltre a fornire

	dei suggerimenti di ordine pratico, richiama concetti come quello della data protection e della privacy, anche in ottica GDPR.
SMART WORKING	Con l'emergenza COVID-19 e il ricorso generalizzato allo smart-working, anche se inteso soprattutto come telelavoro o lavoro da remoto, diventa necessario focalizzare l'attenzione su questo particolare tema. Operare al di fuori "rassicuranti" mura del nostro ufficio, espone tutti gli utenti ad un aumento dei rischi Cyber. Il modulo pone quindi l'accento sui principali punti di vulnerabilità che si incontrano in questa dimensione meno protetta e come si possono mitigare i rischi con comportamenti adeguati che riflettono una maggiore consapevolezza.
SOCIAL COLLABORATION & VIDEO-CONFERENCING	L'emergenza COVID-19 e il rapido ricorso allo smart-working, hanno prodotto un rapido aumento dell'uso degli strumenti di condivisione delle informazioni e di collaborazione, tra i quali citiamo in modo particolare gli strumenti di video-conferenza; un uso che ha travalicato la dimensione professionale per approdare definitivamente in quella personale. Questo modulo mette in evidenza alcune minacce correlate strettamente con il tema della condivisione e della collaborazione, riflettendo sulla necessità di un uso corretto degli strumenti, allo scopo di preservare privacy e sicurezza.
SMISHING & VISHING	Un'altra particolare tecnica di Phishing che colpisce attraverso i sistemi di messaggistica come WhatsApp, Messenger, Telegram, e SMS. Questo modulo, attraverso una serie di esempi concreti, vuole far comprendere all'utente, come anche i sistemi di messaggistica, per certi versi considerati "SICURI", possono nascondere particolari insidie. Mettendo in evidenza come un comportamento non adeguato e poco attento, oltre a mettere in pericolo la nostra sicurezza, e quella della nostra rete relazionale.
SPEAR PHISHING	Si torna a parlare di Phishing richiamando concetti già affrontati in precedenza, partendo dal presupposto che il nostro utente abbia con i precedenti moduli maturato un livello di conoscenza di base per approfondire alcuni argomenti e aumentare la sua capacità di riconoscere un attacco Phishing. In questo modulo, focalizzato sulla necessità di riconoscere un attacco di Spear Phishing e quindi una tecnica sofisticata che colpisce uno specifico individuo o uno specifico gruppo di individui, si pone l'accento su quelle tecniche, che hanno lo scopo di collezionare informazioni sensibili attraverso l'inganno.
RANSOMWARE	È il più subdolo dei MALWARE, quello che provoca più danni e che sottopone individui e organizzazioni ad un ricatto da cui è difficile sfuggire. Attacchi RANSOMWARE sono stati in grado di bloccare l'operatività di business di intere organizzazioni che si sono viste spesso costrette a pagare significative somme, per riprendere il controllo dei dati e delle informazioni. Questa tecnica è sempre più diffusa ed aggressiva e negli ultimi tempi sono stati sempre di più gli attacchi gravi correlati con questa tecnica.
MULTI-FACTOR-AUTHENTICATION	Questo modulo approfondisce i sistemi di autenticazione più evoluti, sia per stimolarne l'uso ove questo è tecnicamente possibile, al fine di rafforzare il livello di sicurezza complessivo degli individui e delle organizzazioni, sia per informare l'utente rispetto alle nuove tecniche con cui gli hacker cercano di superare questi sistemi, facendo leva sul fattore umano. Tra queste si focalizza l'attenzione sia sul cosiddetto Sneaky Phishing, un'evoluzione specifica delle tecniche di Phishing, sia sulla pratica del Sim Swap, con cui i criminali cercano di ottenere fraudolentemente il controllo dello smartphone utilizzato dall'utente.
IoT DEVICE	Siamo sempre più interconnessi e lo saremo sempre di più. L'evoluzione tecnologica ci sta portando verso l'interconnessione totale, che non riguarda più solo le persone, ma anche le cose. Quello che qualche anno fa si sarebbe considerato uno scenario fantascientifico, si sta concretamente realizzando

	sotto i nostri occhi. E questo non riguarda solo la dimensione professionale, ma anche la dimensione privata degli utenti. Elettrodomestici, telecamere, dispositivi indossabili, automobili sempre più intelligenti, anche le cose sono destinate a comunicare sempre di più. La questione si fa per certi versi sempre più affascinante, per altri sempre più inquietante. Ogni dispositivo interconnesso, se non gestito correttamente, diventa un punto di potenziale vulnerabilità per la sicurezza. Questo modulo ci spiega come relazionarci con questo scenario, proponendo comportamenti adeguati che non compromettano il livello di sicurezza della persona e dell'organizzazione.
BLUETOOTH & Wi-Fi	Questo modulo focalizza la sua attenzione su due componenti tecnologiche che sono necessarie per garantire la connessione in movimento e quindi la mobilità delle persone. Sono due componenti strategiche per la trasformazione digitale e per l'innovazione, ma contengono delle insidie che possono essere controllate con un atteggiamento consapevole da parte degli utenti nel loro uso.
INFORMATION CLASSIFICATION	La classificazione delle informazioni è uno dei fattori chiave nella gestione della sicurezza delle informazioni, ma è anche uno dei fattori meno compresi dagli utenti e spesso vissuto come un'inutile imposizione. Eppure, oggi la classificazione delle informazioni è diventata basilare per il rispetto di standard e normative che riguardano la protezione dei dati. Questo modulo, oltre a spiegare il significato e le motivazioni che spingono le organizzazioni a sviluppare processi di classificazione, cerca di far comprendere quanto sia importante adeguare i propri comportamenti in questa direzione. Inoltre, in questo modulo si fa un approfondimento speciale con una categoria particolare di informazioni le PERSONAL IDENTIFIABLE INFORMATION.
DATA PROTECTION	Si torna a parlare di protezione dei dati, con un'accezione che riguarda la sicurezza, e più strettamente la Privacy e la relazione con le varie normative di qualità e di sicurezza delle informazioni, in modo particolare con il GDPR. Questo modulo può essere considerato un richiamo "annuale" del modulo Privacy & GDPR, in una logica di formazione obbligatoria, anche se presenta contenuti originali e più sofisticati rispetto a quelli trattati nel primo livello.
SOCIAL ENGINEERING 2	Alla fine di ogni livello (annualità) si torna a parlare di Social Engineering, e quindi di tecniche di attacco che usano l'inganno e la manipolazione psicologica come base per raggiungere i loro scopi fraudolenti. Questo modulo, prendendo spunto da alcuni esempi tratti dalla realtà, fornisce ulteriori elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli del secondo livello.

VIDEO	
WATERING HOLE	Tutti pazzi per gli sconti. In quest'episodio viene analizzata ancora una volta quella che è una tecnica di attacco cyber mutuata dalla natura: la tecnica della pozza d'acqua (watering hole). Mantenere un atteggiamento vigile e diffidare di strane richieste di informazioni è la strada giusta per proteggersi da questo insidioso attacco.
WHATSAPP SCAMS	Una pesca fruttuosa. In questo episodio, viene raccontata una truffa particolare, che colpisce un dirigente "tecnologicamente impreparato". Si tratta di una delle tante truffe basate su manipolazione psicologica in cui l'hacker, nascosto dietro una falsa identità, riesce a soddisfare i suoi intenti criminali. Nell'era del digitale, essere "tecnologicamente impreparati", non è mai una valida giustificazione per abbassare la guardia.

VISHING & DATA THEFT	Se telefonando. Ormai siamo sempre più abituati a ricevere telefonate da operatori che ci comunicano modifiche unilaterali ai contratti che abbiamo stipulato. La percezione del rischio insito in queste telefonate è diminuita al punto da fornire i dati della carta di credito aziendale ad un operatore che ci comunica modifiche al contratto del conto bancario della nostra azienda! Rispettiamo sempre le regole organizzative sulla gestione dei dati e prestiamo molta attenzione, soprattutto quando abbiamo una responsabilità aziendale legata al nostro ruolo lavorativo. Le conseguenze di una nostra distrazione possono essere molto gravi.
QISHING	Parcheggi pericolosi. In questo episodio viene esaminata una truffa di recente diffusione, che fa leva su un codice sempre più utilizzato: il QR code. Il meccanismo ingannevole di base è lo stesso adottato per il Phishing, con un'esca che viene lanciata per convincere la potenziale vittima a fare un'azione. Per non cadere nell'inganno dovete agire con la massima cautela: a volte, dietro un gesto semplice, si celano delle insidie per la vostra sicurezza.
FAKE WEBSITE	Provare, ma senza dimenticare. Distinguere il vero dal falso nella dimensione digitale può essere un esercizio davvero difficile. Ecco perchè il pericolo di diventare le vittime designate dei criminali Cyber è sempre concreto. Come possiamo proteggerci? Ricorrendo a comportamenti digitali virtuosi, sempre e comunque, soprattutto di fronte a dinamiche simili a quella descritta in questo episodio.
CEO Fraud	Copia con troppa conoscenza. Compromettere gli account aziendali e infiltrarsi negli scambi e-mail delle organizzazioni è la minaccia con cui i cyber criminali popolano gli incubi peggiori dei top manager, soprattutto se gli intrusi sanno perfettamente come mimetizzarsi. Ma questo schema si applica anche a situazioni di vita comune. Nessuno può sentirsi davvero al sicuro.
DATA PROTECTION	Foto ricordo…da dimenticare. Al giorno d'oggi, la semplicità con cui condividiamo dati e informazioni può generare situazioni molto critiche per la nostra Privacy. Seguire alcune semplici accortezze comportamentali, però, può metterci al riparo da condivisioni "indiscrete".
SPEAR PHISHING	Galeotta fu l'e-mail. Il Phishing è una tecnica di attacco informatico che può assumere diverse forme in base al contesto e agli obiettivi degli attaccanti. Gli attacchi di Spear Phishing, come quello narrato in questo episodio, sono generalmente più accurati, ma difficilmente si presentano "perfetti". Il diavolo molto spesso si nasconde nei dettagli! Fai attenzione a tutti gli elementi delle comunicazioni che ricevi.
FAKE NEWS	Oltre le apparenze. Questo episodio approfondisce la minaccia che si nasconde dietro le false notizie, che ormai spopolano indisturbate nella rete. Prima di credere ad una notizia sensazionale trovata sul web, dobbiamo sottoporla ad una radiografia accurata. Un comportamento critico e attento può metterci al riparo da conseguenze molto spiacevoli.
PHARMING	Una donazione "sbagliata". Questo episodio mette in evidenza una tecnica di attacco particolarmente subdola, che nella creatività degli specialisti della Cybersecurity ha assunto un nome particolare: PHARMING. Ma cos'è il PHARMING? Qualcuno sostiene che non sia altro che un PHISHING senza esca. Approfondiamo insieme le precauzioni da prendere per ridurre al minimo le probabilità di essere attaccati.
PRIVACY	Post Pericolosi. Nell'era della condivisione attraverso i Social, esiste ancora la Privacy? Questo episodio racconta la storia di un candidato "scartato" da una selezione, a causa di un post pubblicato sui suoi profili social. Un monito per i giovani, ma anche per i meno giovani, visto che nella dimensione social le barriere anagrafiche non contano. Una riflessione sul fatto "che la rete non perdona" e che tutto quanto affermiamo e pubblichiamo sui social sopravvive addirittura a noi stessi.

SHARED DEVICES	Una vacanza "non proprio low cost". Il "succo" di questa storia è rappresentato dall'importanza che i nostri dispositivi hanno assunto sia nella sfera privata che in quella professionale. Nel "triangolo delle Bermuda" rappresentato da Smartphone, Tablet e Computer, possiamo trovare tutta la nostra vita personale e professionale. Per questo dobbiamo essere molto attenti alle modalità con cui usiamo questi strumenti. L'ingenuità commessa dal nostro protagonista che per fare un'operazione riservata si è affidato ad un dispositivo "prestato" da una persona conosciuta da poco, ci deve far riflettere sui rischi della dimensione digitale. Se ci hanno insegnato a non accettare caramelle dagli sconosciuti, dobbiamo applicare questo insegnamento anche ai dispositivi elettronici.

VALUTAZIONE DI APPRENDIMENTO

Ogni lezione è corredata da test di valutazione del singolo livello di apprendimento.

La valutazione prevede inoltre verifiche random per evidenziare l'implementazione del livello delle competenze acquisite confrontate con quelle inizialmente possedute e relative alla individuazione di attacchi in situazioni simulate.

ASSISTENZA TECNICA

In caso di difficoltà di accesso alla piattaforma l'utente dovrà rivolgersi alla
UOC Flussi Informativi, ICT e Innovazioni di Processo
Tel: 0773 655 3222
Mail: *informatica@ausl.latina.it*

Ove dovessero verificarsi problemi nella fruizione del corso, si prega di contattare la Accenture Security, Gestore della piattaforma, ai recapiti indicati sulla Home Page della piattaforma stessa.