Suite Cybersecurity

ABISERVIZI ABI FORMAZIONE

Suite Cybersecurity

CONTENUTI

I corsi della suite, multimediali e interattivi, offrono esempi di truffe informatiche e casi pratici di cybersecurity e descrivono i principali e più attuali trend di minaccia dei cyber criminali per favorire la consapevolezza dei rischi, la capacità di riconoscerli e di applicare le precauzioni e i mezzi di difesa più opportuni. Ricchi di esempi, didascalici e divulgativi, i corsi forniscono in modo semplice e diretto le regole da seguire quotidianamente per sviluppare buone prassi di “cyber hygiene”.

I contenuti sono a cura di Giorgio Sbaraglia, Cybersecurity Consultant e socio Clusit.

I corsi rispondono agli standard del Regolamento IVASS 40/2018.

Suite Cybersecurity

La suite è articolata nei seguenti corsi:

Cybersecurity: un gioco di squadra	Intro	15 minuti
Perché la cybersecurity è diventata così importante	IVASS	50 minuti
Le modalità più utilizzate di attacco informatico. Social engineering e phishing	IVASS	1 ora e 10 minuti
Gli attacchi attraverso la posta elettronica	IVASS	45 minuti
I ransomware: la minaccia oggi più temibile	IVASS	1 ora
Malware su dispositivi mobili	IVASS	45 minuti
Messaggistica istantanea: ci possiamo fidare?	IVASS	35 minuti
Imparare a usare le password	IVASS	1 ora

Suite Cybersecurity

DESTINATARI
Operatori di filiale bancaria, di agenzia assicurativa, di help desk, di contact centre, di back office

DURATA
6 ore

FORMAT
Corsi multimediali e interattivi, orientati a modelli di coinvolgimento attivo dell'utente

IL TRACCIAMENTO
I corsi fruiti tramite **LMS di ABIFormazione,** indipendentemente dai formati, inviano alla piattaforma i dati di tracciamento utili per la produzione della reportistica, compresa quella **richiesta da FBA**, conforme alla **Circolare ANPAL n. 4 del 28.12.2020.** I corsi predisposti per le piattaforme LMS delle aziende clienti sono realizzati secondo lo **standard SCORM 1.2**

Cybersecurity: un gioco di squadra

ABISERVIZI ABI FORMAZIONE

Cybersecurity: un gioco di squadra

CONTENUTI

Se il cyber crime fosse una nazione e il suo giro d'affari fosse il suo PIL - nel 2021 è stato stimato in 6.000 miliardi - la sua economia sarebbe al terzo posto nel mondo dietro solo a USA e Cina.
E corrisponderebbe a circa il triplo del PIL dell'Italia...

OBIETTIVO

… pochi preziosi minuti dedicati all'introduzione al tema della cybersecurity e all'importanza della responsabilizzazione di tutti all'interno dell'azienda, soprattutto in un contesto decisamente segnato dagli ultimi anni di pandemia

DURATA:

15 minuti di fruizione lineare

Cybersecurity: un gioco di squadra

INDICE

Perché la cybersecurity è diventata così importante

ABISERVIZI ABI FORMAZIONE

Perché la cybersecurity è diventata così importante

CONTENUTI

Nessuno oggi può prescindere dal considerare la cybersecurity come elemento strategico per la difesa dei propri dati, aziendali o personali: la questione non è quella di sapere “se saremo attaccati” ma solo “quando”.
Non importa se siamo grandi o piccoli, privati o aziende: il rischio di attacco è sempre dietro l’angolo.
Il web è diventato un luogo pericoloso? Possiamo difenderci

OBIETTIVO

Illustrare le caratteristiche, il ruolo e la rilevanza della cybersecurity nella protezione dei dati in azienda e descrivere le misure di sicurezza e prevenzione del rischio informatico adottate in Italia e Europa

DURATA

50 minuti di fruizione lineare

Perché la cybersecurity è diventata così importante

INDICE

Le modalità più utilizzate di attacco informatico. Social engineering e phishing

ABISERVIZI
ABI FORMAZIONE

Le modalità più utilizzate di attacco informatico. Social engineering e phishing

CONTENUTI

Malware, escalating privilege, backdoor, DDoS, drive by download, phishing e soprattutto social engineering: sono gli attacchi informatici più diffusi verso siti web, servizi FTP, posta elettronica, dispositivi mobili, reti aziendali.
Prevenire le mosse dell'avversario aiuta a combattere il nemico: una strategia militare vecchia come il mondo, che oggi può essere applicata anche all'ambito informatico

OBIETTIVO

Descrivere cause, effetti e metodologie degli attacchi informatici con particolare riferimento al social engineering e al phishing

DURATA

1ora e 10 minuti di fruizione lineare

Le modalità più utilizzate di attacco informatico. Social engineering e phishing

INDICE

Gli attacchi attraverso la posta elettronica

ABISERVIZI ABI FORMAZIONE

Gli attacchi attraverso la posta elettronica

CONTENUTI

Tutti noi mandiamo e riceviamo e-mail.
La posta elettronica è lo strumento informatico più utilizzato nelle aziende di tutto il mondo e dai singoli individui per lo scambio di messaggi, file e allegati di ogni genere.
Ma la posta elettronica è anche uno dei canali più sfruttati dal cybercrime.
Per veicolare malware o truffe, come la «business e-mail compromise» che può generare danni economici e reputazionali molto gravi per le organizzazioni.
Anche in questo caso, non fidarsi e attuare i comportamenti corretti consente di mitigare i rischi cyber anche per gli attacchi più sofisticati

OBIETTIVO

Descrivere le caratteristiche degli attacchi informatici veicolati dalla posta elettronica (con un focus dedicato alla business e-mail compromise - BAC), i rischi e i danni che possono comportare per le aziende e gli strumenti informatici di difesa attualmente esistenti

DURATA

45 minuti di fruizione lineare

Gli attacchi attraverso la posta elettronica

INDICE

I ransomware: la minaccia oggi più temibile

ABISERVIZI ABI FORMAZIONE

I ransomware: la minaccia oggi più temibile

CONTENUTI

Il 2017 è l'anno di Wannacry, il ransomware che ha infettato centinaia di migliaia di computer in 150 paesi nel giro di poche ore, sequestrando i file degli utenti e richiedendo un riscatto in criptovaluta per sbloccarli.
Dietro all'industria del ransomware non ci sono semplici hacker, ma vere e proprie organizzazioni criminali con un alto livello di competenza e di efficienza.
Per questo è importante conoscere le modalità con cui questi malware si propagano per applicare al meglio le regole di "cyber igiene" che ci possono proteggere

OBIETTIVO

Descrivere le caratteristiche dei ransomware, le modalità d'attacco, le misure di prevenzione per evitarli e le azioni da intraprendere in caso di attacco subito

DURATA

1 ora di fruizione lineare

I ransomware: la minaccia oggi più temibile

INDICE

Malware su dispositivi mobili

ABISERVIZI ABI FORMAZIONE

Malware su dispositivi mobili

CONTENUTI

Nell’ottobre del 2016 il traffico internet da dispositivi mobili, generato in gran parte da smartphone e tablet, ha superato quello da dispositivi fissi.
Uno smartphone oggi è la più grande banca dati di una persona.
Un bersaglio allettante per i cybercriminali che grazie a tecniche sempre nuove e canali di trasmissione sempre più numerosi rendono i loro attacchi particolarmente insidiosi.
Essere consapevoli di queste minacce e adottare una serie di accorgimenti per prevenirle può fare la differenza

OBIETTIVO

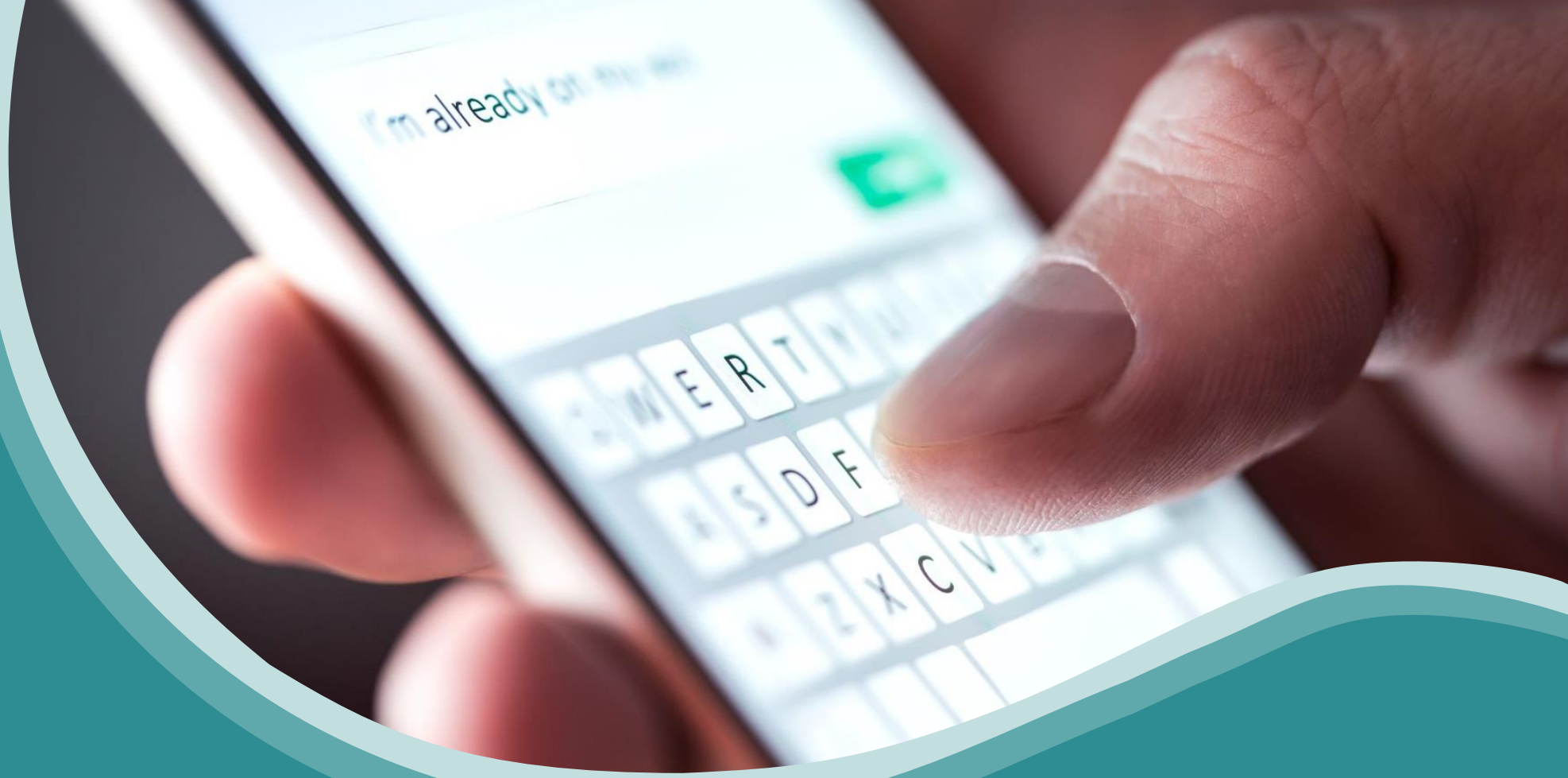
Descrivere i rischi connessi all'utilizzo di dispositivi mobili, le principali modalità d'attacco utilizzate dal cybercrime e le misure di prevenzione per difendersi da un possibile cyber attacco

DURATA

45 minuti di fruizione lineare

Malware su dispositivi mobili

INDICE



Messaggistica istantanea: ci possiamo fidare?

ABISERVIZI ABI FORMAZIONE

Messaggistica istantanea: ci possiamo fidare?

CONTENUTI

Sempre più persone utilizzano lo smartphone per scambiare informazioni in modo rapido, condividere foto, inviare messaggi vocali, tramite applicazioni di messaggistica istantanea, come WhatsApp, Facebook Messenger o Telegram.
Il traffico generato da questo scambio massivo ha reso i sistemi di messaggistica istantanea un target molto appetibile per il cybercrime.
Molto dipende dai nostri comportamenti: impariamo a utilizzare questi strumenti in modo sicuro

OBIETTIVO

Descrivere i rischi correlati all'utilizzo delle applicazioni di messaggistica istantanea (IM), le principali tipologie di truffe e i sistemi di messaggistica ritenuti più sicuri

DURATA

35 minuti di fruizione lineare

Messaggistica istantanea: ci possiamo fidare?

INDICE

Imparare a usare le password

ABISERVIZI
ABI FORMAZIONE

Imparare a usare la password

CONTENUTI

Viviamo immersi in un ambiente digitale costituito da computer, smartphone e tablet, in cui conserviamo moltissimi dati, alcuni particolarmente rilevanti.
Da questo punto di vista, è corretto considerare le password come le chiavi di casa.
Qualcuno oggi le lascerebbe attaccate alla serratura?
Probabilmente no. Allo stesso modo, dovremmo avere la stessa attenzione per le nostre password che, invece, spesso lasciamo inconsapevolmente nelle mani degli hacker

OBIETTIVO

Conoscere le principali regole per la corretta gestione delle password e descrivere l'utilizzo di strumenti software e le misure precauzionali per la protezione efficace degli account

DURATA

1 ora di fruizione lineare

Imparare a usare la password

INDICE

Suite Cybersecurity

REQUISITI TECNICI

cuffie o altoparlanti - Risoluzione minima: 1024x768 pixel - Connessione a internet: ADSL o superiore
HTML5
Windows: Microsoft Edge (versione corrente), Google Chrome (versione corrente), Firefox (versione corrente)
Mac: Safari (versione corrente), Google Chrome (versione corrente), Firefox (versione corrente)
Mobile: Safari e Google Chrome per iOS 10 o superiore, Google Chrome per Android 4.4 o superiore

abiformazione.it
abilearning.it

Oltre 20 anni insieme.

Un viaggio nel mondo della formazione, orientato allo sviluppo delle competenze di migliaia di persone nelle banche, negli intermediari finanziari e assicurativi, nelle aziende e negli enti pubblici.

CONTATTI:

gestioneclienti@abisevizi.it
06.6767.640
Salita di San Nicola da Tolentino, 13 00187 – Roma

UNI EN ISO 9001:2015 per i Settori IAF 37, 35, 08

ABISERVIZI ABI FORMAZIONE