Proofpoint

Biztonságtudatossági képzés

Fejlessze játékosan, izgalmasan munkatársait!

Biztonságtudatossági képzés egyedülálló és hatékony megközelítésben

A Proofpoint interaktív képzési moduljait úgy állították össze, hogy segítsék Önöket a megfelelő képzés, tematika és időkeret összeállításában.

- A leckék rövidek és lényegre törőek. Minden egyes modul elvégzéséhez átlagosan **5-15 perc** szükséges.
- A mobiltelefonra optimalizált felület lehetővé teszi a felhasználók számára, hogy a képzést **bárhol, bármikor** internethez csatlakoztatott eszközön igénybe vehessék.
- Az oktatási tematika egymásra épülő részegységeken alapul, amely könnyedén ütemezhető akár 1 éves időszakra vonatkozóan, arányosan szétosztva.
- A modulok magyarul is rendelkezésre állnak. A professzionális színvonalon lefordított és helyi igényekre szabott tartalom leköti a munkavállalók figyelmét és folyamatosan a rájuk leselkedő veszélyek felismerésére készteti őket.
- Folyamatos frissítések biztosítják, hogy a képzés naprakész legyen.
- A játékos elemek, az interaktivitás folyamatosan fenntartja a felhasználók érdeklődését. A munkavállalók állítják be saját előrehaladásuk ütemét és mindvégig visszacsatolást kapnak.

Biztonságos e-mail használat

ALAPCSOMAG

Bevezetés az adathalászatba

Megtanítja a felhasználókat arra, hogyan lehet felismerni az e-mailes csapdákat és elkerülni az adathalász támadásokat.

Veszélyes csatolmányok elkerülése

A veszélyes e-mail csatolmányok azonosítására és elkerülésére fókuszál.

Veszélyes linkek elkerülése

Ismerteti a széles körben elterjedt e-mailes csapdákat és azt, hogyan kerülhetjük el a veszélyes linkeket.

Bejelentkezési adatok védelme

Megtanítja a felhasználókat arra, hogyan tudják azonosítani és elkerülni azokat az átveréseket, amelyek célpontjai személyes vagy érzékeny adatok.

Levelezés védelmi eszközök

Felkészíti a felhasználókat, hogyan tudják megvédeni magukat az adathalász átverésekkel szemben a levelezés-védelmi eszközök együttes alkalmazásával.

E-mail biztonság mobil eszközökön

Feltárja, hogyan azonosítsuk és kerüljük el az adathalász e-maileket a mobil eszközökön.

Célzott adathalász fenyegetések

Megtanítja a felhasználókat arra, hogy ismerhetők fel és kerülhetők el a célzott adathalász támadások.

Jelszóvédelem

A jelszavakon túl

Ismerteti, hogyan használjuk a PIN-kódokat és a jelszavakat eszközeink és fiókjaink biztonságossá tételére.

Többfaktoros hitelesítés (MFA)

Segítséget nyújt abban, hogyan tehetjük felhasználói fiókjainkat többtényezős hitelesítéssel biztonságosabbá.

A jelszavak kezelése

Bemutatja a jelszavak biztonságos kezelésének legjobb példáit.

Jelszavakkal kapcsolatos előírások

Megtanítja a felhasználókat arra, hogyan tudnak a szervezeti előírásoknak megfelelő jelszavakat létrehozni.

Biztonságos e-mail használat

HALADÓ

E-mail-védelmi eszközök

Megtanítja a felhasználókat, hogyan tudják megvédeni magukat az adathalász átverésekkel szemben e-mail védelmi eszközök együttes alkalmazásával.

E-mail biztonság mobil eszközökön

Bemutatja, hogyan azonosítsuk és kerüljük el az adathalász e-maileket a mobil eszközökön.

Adathalász támadások

Megtanítja a felhasználókat arra, hogy ismerhetőek fel és kerülhetőek el a célzott adathalász támadások.

Belső fenyegetések

A bennfentes fenyegetésről

Bevezet a bennfentes fenyegetés fogalmába és bemutatja az ellene való védekezés legjobb gyakorlatait.

Rosszindulatú bennfentes fenyegetések

A valós életből vett példákon keresztül mutatja be a felhasználók számára, hogyan enyhíthető a rosszindulatú fenyegetések hatása.

Nem szándékos cégen belüli fenyegetés

Végigvezeti a felhasználókat azokon a veszélyt hordozó lehetőségeken, amelyekkel a munkavállalók nem szándékos fenyegetést okozhatnak.

A személyazonosításra alkalmas információk (PII)

PII a gyakorlatban

Különböző lehetséges forgatókönyveket mutat be a felhasználóknak, melyen keresztül megtanulják, hogyan befolyásolják a különböző döntések a PII-k megóvására irányuló képességünket.

A PII alapismeretek

Megtanítja a felhasználókat arra, hogyan védjék meg saját magukkal, a vállalatukkal és ügyfeleikkel kapcsolatos bizalmas információkat.

Fiókjai rendeltetésszerű működésének védelme

A veszélyeztetett fiókok azonosítása

Azonosítsa, hogyan és miért gátolják a támadók a fiókok optimális és rendeltetésszerű működését. Tanuljon a legjobb gyakorlatokról, amelyekkel elkerülheti a működésében akadályozott fiókkal kapcsolatos olyan veszélyeket, mint az e-mailes csalás.

A készülékeket érintő veszélyek csökkentése

Bemutatja, hogy a támadók hogyan akadályozzák a készülékek optimális és rendeltetésszerű működését. Tanuljon a legjobb gyakorlatokból, hogy elkerülje a készülék működésének káros hatásait vagy az ezzel járó csalásokat.

ÖSSZEFOGLALÓ

Biztonságtudatossági képzések

Invitech ICT Services Kft. | 2040 Budaörs, Edison utca 4. | Info-vonal: 08 80 82 00 82 | kapcsolat@invitech.hu | www.invitech.hu

További képzések

Adatvédelem és megsemmisítés

Felkészíti a munkavállalókat arra, hogyan használják biztonságosan az adathordozó eszközöket és hogyan semmisítsék meg megfelelően az érzékeny adatokat.

E-mail biztonság

A veszélyes e-mail csatolmányok azonosítására és elkerülésére fókuszál.

Áttekintés az európai általános adatvédelmi rendeletről (GDPR)

Bevezeti a felhasználókat a személyes adatok Európai Általános Adatvédelmi Rendelet szerinti védelmébe.

GDPR a gyakorlatban

Felkészíti a felhasználókat, hogyan alkalmazzák a GDPR-ben meghatározott fogalmakat a mindennapi helyzetekre és döntésekre.

Mobil applikációk biztonsága

Megtanítja a felhasználókat, hogyan ítéljék meg a mobil alkalmazások biztonságát.

Mobil készülékek biztonsága

Ismerteti a fizikai és technikai óvintézkedéseket, amelyekkel megvédhetők a készülékek és az adatok.

Fizikai biztonság

Megtanítja a felhasználókat arra, hogyan tartsák a személyeket, a területeket és az eszközöket nagyobb biztonságban.

Védett egészségügyi információk (PHI)

Megtanítja a munkavállalókat, miért és hogyan kell megóvniuk a védett egészségügyi információkat.

További képzések II.

Védekezés zsarolóprogramok ellen

Megtanítja a felhasználókat, hogyan ismerjék fel és akadályozzák meg a zsarolóprogramok általi támadásokat.

A közösségi hálózatok biztonságos használata

Megmutatja a felhasználóknak, hogyan lehet a közösségi hálózatokat biztonságosan és felelősen használni.

Biztonságosabb web-böngészés

Arra összpontosít, hogyan maradhatunk biztonságban az Interneten a kockázatos magatartás és az gyakori csapdák elkerülésével.

Biztonság az irodán túl

Bemutatja a felhasználóknak, hogyan kerülhetők el a gyakori biztonsági hibák, mialatt otthon vagy útközben dolgoznak.

Biztonsági alapok

Feltárja azokat az általános biztonsági kérdéseket, amelyekkel a napi üzleti vagy személyes tevékenységek során találkozunk.

Biztonsági alapok – Vezetőknek

Megtanítja a felhasználókat, hogyan ismerjék fel és kerüljék el azokat a fenyegetéseket, amelyekkel a felsővezetők munkájuk során és otthon találkoznak.

Pszichológiai manipuláció

Megtanítja a felhasználókat, hogyan ismerjék fel és kerüljék el a pszichológiai manipuláción alapuló átveréseket.

Biztonság utazás közben

Feltárja, hogyan tartsuk adatainkat biztonságban, amikor repülőtereken, szállodákban és egyéb közterületeken dolgozunk.

További képzések III.

A PCI DSS adatbiztonság megértése

Bemutatja a felhasználóknak, hogyan ismerjék fel a figyelmeztető jeleket és javítsák hitelkártyájukon lévő adataik biztonságát.

URL képzés

Ismerteti, hogyan szűrjük ki a hamis URL-eket.

Az USB eszköz biztonsága

Megtanítja a felhasználókat, hogyan védjék magukat, adataikat és a rendszereket, amikor USB eszközöket használnak.

Munkahelyi biztonság a gyakorlatban

Ez a modul megerősíti az irodai biztonság kulcselemeit és olyan témákat ölel fel, mint a pszichológiai manipuláció, a bennfentes fenyegetések és a kifigyelés.

További információért, látogasson el az alábbi címre:
https://www.invitech.hu/informaciobiztonsag-webinar/

Csomagok

ALAP CSOMAG **Megtanítja a felhasználókat védekezni az adathalász támadások ellen. Átfogó és hatékony tudást biztosít az adathalászat ellen.**	TELJES CSOMAG **A teljeskörű képzési módszertant magában foglalja, mely jelentősen hozzájárul a felhasználói gondolkodásmód megváltoztatásához.**
Szimulált adathalász támadások	Szimulált adathalász támadások
Képzés-menedzsment rendszer (SCORM) telepítése	Képzés-menedzsment rendszer (SCORM) telepítése
8 db tréning modul: 1. Biztonságos e-mail használat (alap szint) 2. Biztonságos e-mail használat (haladó szint) 3. Levelezés védelem 4. URL tréning 5. Pszichológiai manipuláció kivédése 6. Védekezés zsarolóprogramok ellen 7. Anti-Phishing Phil™ - Interkatív játék 8. Anti-Phishing Phyllis™ - Interaktív játék	Az összes tréning modult biztosítjuk
PhishAlarm® E-mailes támadások jelzésére szolgáló gomb	PhishAlarm® E-mailes támadások jelzésére szolgáló gomb
PhishAlarm Analyzer A fenyegetések fontosságának prioritási sorrendbe állítása	PhishAlarm Analyzer A fenyegetések fontosságának prioritási sorrendbe állítása
Végfelhasználói szinkronizálás Active Directory-val (AD)	Végfelhasználói szinkronizálás Active Directory-val (AD)
	CyberStrength® Tudás-felmérés
	ThreatSim® USB szimuláció
	Oktatási anyagok
	Tudatosságnövelő videó-kampányok

További tulajdonságok és előnyök

Jelentések és analitikai elemzések	Multinacionális támogatás	Végfelhasználói hozzáférés
• Automatizált jelentési funkció • Paraméterek tucatjainak felhasználásával az adatok dinamikus szűrése • XLS-be és CSV formátumba exportálható • Összehasonlítás más Proofpoint ügyfelekhez való összehasonlítással, beleértve az iparág-specifikus adatokat is	• A felmérések és a képzés anyaga 35+ nyelven érhető el • A nemzetközi időzónák támogatása • Regionális adattárolás és adatvédelmi funkciók • A régióra jellemző domain-ek, nevek és hivatkozások használata	• Egyszeri regisztráció elegendő a Biztonsági Oktatási Platformunkhoz • Az interaktív képzési modulok mobilon is elérhetőek • Megfelelés az 508. Szakasz és a WCAG 2,0 AA megfelelési követelményeinek

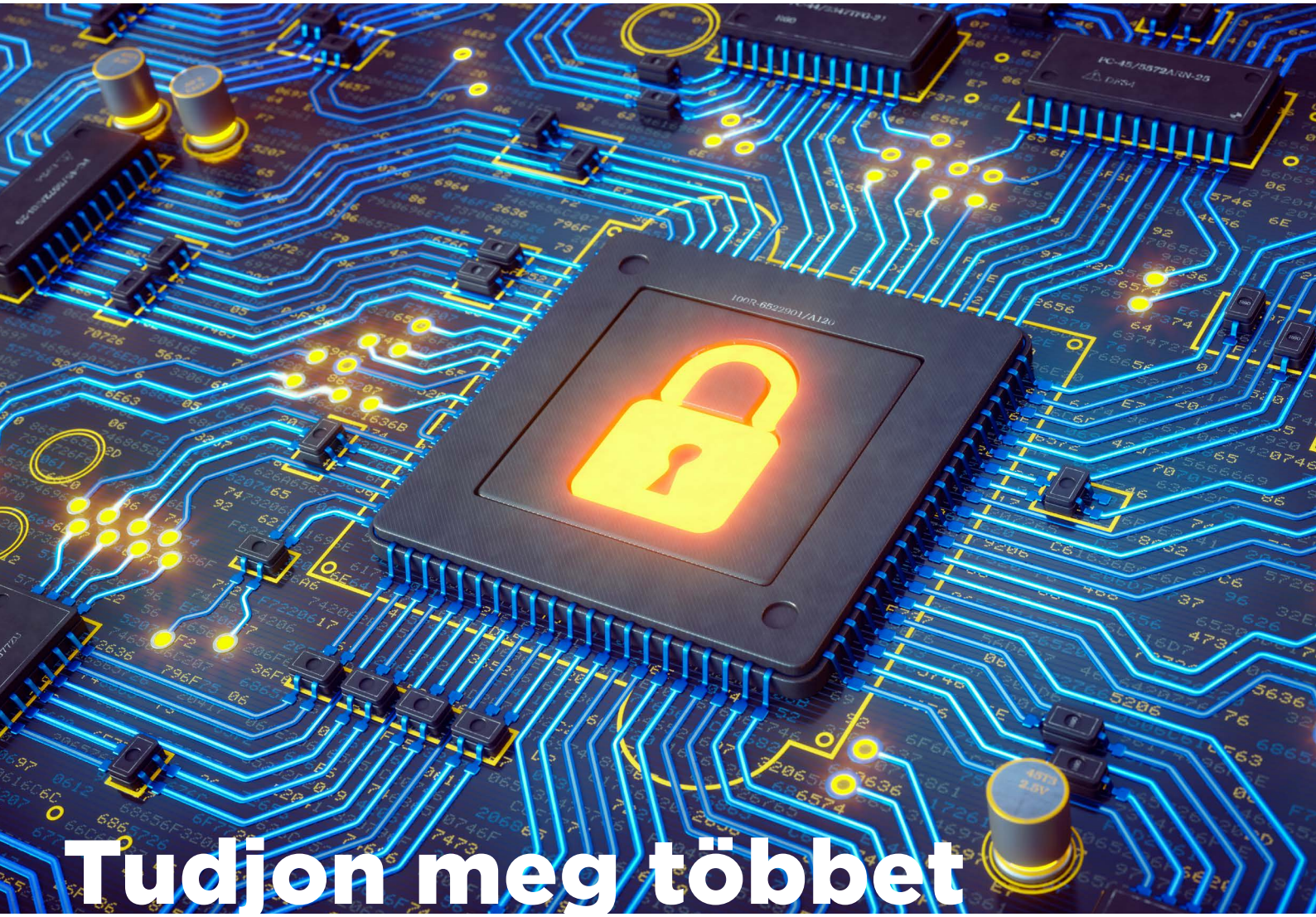
Adminisztráció és biztonság	Támogatás és szolgáltatások	Műszaki tanúsítványok
• Licenccel rendelkező végfelhasználók számára a felmérések, a képzés és jelentési funkció korlátlan használata • Kétfényezős hitelesítés rendszergazdák számára • A jelszó újbóli használatának korlátozása és kizárás meghiúsult bejelentkezési kísérleteket követően • A rendszergazdai jelszó-policy személyre szabása Biztonsági Oktatási Platformunkban	• Támogatás e-mailen, telefonon és élő chat-elésen keresztül • Online közösségi tudásbázissal, ötletekkel, beszélgetésekkel • Az ügyfélhez rendelt Ügyfélkapcsolati Menedzser biztosítása • Hozzáférés a legjobb gyakorlatokról szóló széleskörű dokumentációhoz	• Éves, független harmadik fél által (TRUSTe) végzett adatvédelmi felmérés • Saját tanúsítás az EU-USA Adatvédelmi Pajzzsal és a Svájci-USA Adatvédelmi Pajzs kerettel • Cloud Security Alliance (Felhőbiztonsági Egyesülés) STAR önértékelés • Okta integrációs partner az egyszeri regisztrációhoz • FedRamp tanúsítás

Kiegészítések a csomagokhoz

Menedzselt szolgáltatások	További integrált szolgáltatások és termékek
• Testreszabott biztonságtudatossági és képzési programok • Személyre szabott támogatás • Átfogó, 8 elemet tartalmaz funkció	• Célzott adathalász fenyegetések (CLEAR) megoldás

* Valamennyi képzési modul reszponzív, mobilra optimalizált, kivéve: az URL képzés, a Mobil alkalmazások biztonsága, az E-mail biztonság, az Anti-Phishing Phil és az Anti-Phishing Phyllis modulok.

invitech



Tudjon meg többet

További információ:

https://www.invitech.hu/informaciobiztonsag-webinar/