datasense

ON-LINE ŠKOLENÍ
KYBERNETICKÁ BEZPEČNOST

V poslední době stoupá počet kybernetických útoků nejen na veřejnou správu, ale i na společnosti v soukromém sektoru, a je třeba se bránit. Více než 90% všech těchto útoků začíná e-mailem a antivirové programy, do kterých společnosti investují nemalé finanční prostředky, už bohužel nestačí. Útočníci začali cíleně napadat zaměstnance a spoléhají, že některý z nich udělá ve chvilce nepozornosti chybu - **KLIKNE!**

Je důležité naučit zaměstnance rozpoznat riziko hrozby, jako jsou phishingové útoky, nebezpečné odkazy, škodlivé přílohy či žádosti o osobní údaje, které by mohly být v budoucnu zneužity.

Průzkumy dokazují, že standardní školení, konající se jednou za rok, není dostatečně efektivní a jeho přínos v čase velmi rychle mizí. Kontinuální, pravidelné vzdělávání, které účastníky učí osvědčené postupy, jak se kybernetickým rizikům bránit, zvyšuje připravenost organizace a jednotlivců proti potenciálním útokům.

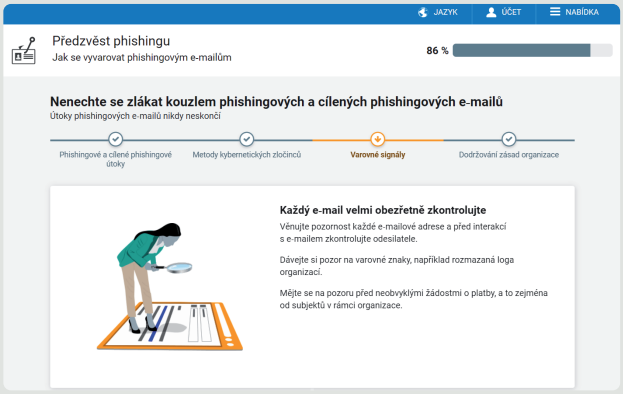
Díky našemu on-line školícímu programu ve vámi zvoleném jazyce se vaši zaměstnanci během krátkých, cíleně zaměřených lekcí, naučí rozpoznat riziko hrozby a tím chránit data celé organizace.

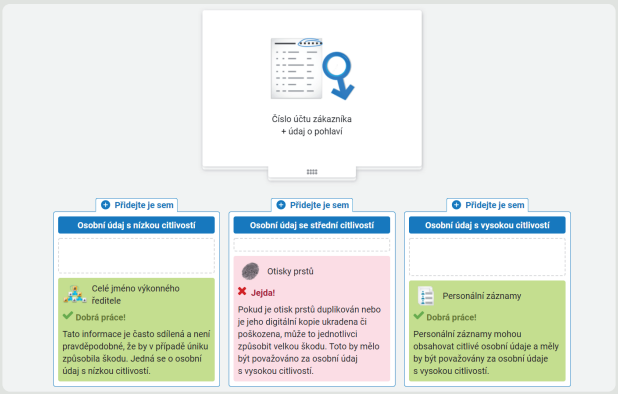
TÉMATICKÉ OKRUHY ŠKOLENÍ

- **Phishing** - seznámení se s druhy phishingových e-mailů, jakým způsobem je rozpoznat a jak reagovat. Jak prověřit nebezpečné odkazy URL a rozpoznat, které jsou nebezpečné a škodlivé.
- **GDPR** - typy osobních informací, jakým způsobem shromažďovat citlivá data, správné zacházení s nimi a jejich správná likvidace.
- **Správa hesel** - nezbytná součást ochrany pracovních i soukromých dat. Základy bezpečného používání hesel, jak vytvořit silná a zároveň dobře zapamatovatelná hesla.
- **Zabezpečení mobilních zařízení** - zabezpečení mobilních telefonů, tabletů a USB disků před krádežemi. Vytváření správných PIN kódů, jak rozpoznat nebezpečné aplikace, nebezpečí veřejných sítí, atd.
- **Sociální inženýrství** - taktiky sociálních inženýrů, jak se nejlépe chránit, a jak těmto útokům zabránit.
- **Fyzické zabezpečení** - zajištění fyzického zabezpečení nejen na pracovišti, ale i doma, či na cestách. Prevence proti jeho narušení. Zabezpečení techniky.

Cloudová platforma, přes kterou se školení realizuje, obsahuje **interaktivní výukové moduly, jejichž délka trvání je 10 – 20 min.** Přehledné lekce s herními prvky jsou zasílány všem účastníkům školení, kteří mají předem stanovené časové rozmezí na jejich splnění.

V průběhu každého výukového modulu jsou kontrolní otázky a závěrečný kvíz, který pomáhá účastníkům kurzu ověřit si naučené poznatky.





Vámi zvolená edice a délka vzdělávacího programu zahrnuje i simulované phishingové útoky prověřující účinnost školení, pravidelný reporting a naši odbornou podporu.

V případě zájmu o bližší informace nás neváhejte kontaktovat!

Tereza Čejková
Sales Representative
M: +420 608 822 266
E: tereza.cejkova@datasense.cz

Božetěch Brablc
Managing Partner
M: +420 731 153 108
E: bb@datasense.cz

Alžběta Nováková
Sales Representative
M: +420 601 323 425
E: alzbeta.novakova@datasense.cz

www.bezpeci.info