ŠKOLENÍ KYBERNETICKÉ BEZPEČNOSTI

CÍL ŠKOLENÍ

Cílem tohoto školení je zvýšit bezpečnostní povědomí uživatelů formou jejich seznámení s nejnovějšími hrozbami v kybernetickém prostoru a možnostmi ochrany proti těmto hrozbám, naučit je zásadám bezpečného zacházení s informacemi a výpočetní technikou v kyberprostoru a zároveň odpovědnosti za svěřené informace a výpočetní techniku.

CÍLOVÁ SKUPINA

Cílovou skupinou pro tato školení jsou všichni uživatelé výpočetní techniky bez rozlišení odbornosti a organizačního zařazení.

PŘÍNOSY

Hlavním přínosem pro účastníky školení je:

rozšíření znalostí uživatelů o způsobech ochrany informací a výpočetní techniky před útoky z Internetu i útoky vedené formou sociálního inženýrství a také o bezpečném způsobu zacházení s informacemi. Tento přínos by měl být patrný při porovnání výsledků úvodního a závěrečného testu.

Hlavním přínosem pro organizaci je:

zvýšení úrovně znalostí uživatelů a v jeho důsledku snížení bezpečnostních rizik plynoucí z typických chyb a nesprávného chování uživatelů.

OBSAHOVÁ NÁPLŇ

- **Úvodní znalostní test**

  Krátký úvodní znalostní test ověří počáteční úroveň znalostí uživatelů v oblasti internetové bezpečnosti a bezpečného zacházení s informacemi.

- **Proč se zabývat bezpečností informací**

  Seznámení s hlavními důvody a principy ochrany informací a hlavními příčinami ohrožení informací.

- **Aktuální hrozby pro informace**

  Přehled kybernetických hrozeb z poslední doby. Nebezpečnost kyberprostoru bude doložena i vybranými statistikami. Seznámení s vývojem kybernetické kriminality a motivací útočníků, příklady cen zcizených dat na černém trhu.

- **Škodlivý software**

  Stručný přehled typů škodlivého software a jeho funkcí. Seznámení se způsoby napadení počítače škodlivým softwarem. Popis vybraných speciálních typů útoku (QR kódy, MITB).

- **Mobilní bezpečnost**

  Rizika a ochrana informací při použití mobilních prostředků výpočetní techniky. Srovnání zranitelností mobilních platforem.

- **Sociální inženýrství**

  Principy a techniky sociálního inženýrství. Způsoby obrany proti tomuto typu útoku. Video o útoku s využitím sociálního inženýrství.

- **Obecné bezpečnostní zásady**

  Obecné zásady ochrany před kybernetickými hrozbami i hlavní zásady bezpečné manipulace s informacemi. Požadavky na silné heslo, způsob jeho vytvoření a bezpečné zacházení s hesly.

- **Sociální sítě**

  Hlavní rizika sociálních sítí. Děti a nevyškolení uživatelé jako nejohroženější skupina uživatelů Internetu. Kde se dá najít pomoc nebo dobrá rada.

- **Shrnutí**

  Shrnutí hlavních zásad ochrany před kybernetickými hrozbami.

- **Závěrečný test**

  Zopakování úvodního testu pro porovnání vstupní a výstupní úrovně znalostí uživatelů.

- **Diskuse**

  Volná diskuse s uživateli o tématech, která je v oblasti kybernetické bezpečnosti zajímají.

REALIZACE

Školení je realizováno interaktivní formou, přičemž je použita kombinace výkladu s využitím prezentace v powerpointu a vzdělávací videa s aktivním zapojením uživatelů formou diskuse a prezentace jejich názorů. Na začátku i na konci je ověřena úroveň znalostí uživatelů krátkým testem.

DOKUMENTACE

Účast na školení bude dokumentována prezenční listinou. Každý účastník vyplní na úvod a na závěr školení krátký test znalostí z oblasti kybernetické bezpečnosti. Všichni účastníci obdrží na konci školení "Desatero bezpečnostních zásad uživatele IT" a následně také certifikát o absolvování školení. Objednatel obdrží analýzu obecné znalosti uživatelů v kybernetické bezpečnosti a doporučení lektora pro organizaci.