IT SECURITY PRO PODNIKOVÉ ŘÍZENÍ

Dnes již každý z nás běžně pracuje v práci s internetem. Znáte však zásady bezpečného využívání počítačů? Víte, na co si dát na Internetu pozor? Víte, jak se bezpečně pohybovat a komunikovat na Internetu? Víte, jak zabezpečit počítač, datová média nebo datovou síť před účinky škodlivých programů? Umíte zálohovat svoje data na počítači? Pokud je většina vašich odpovědí na předchozí otázky záporná, pak je tu školení přímo pro Vás!

Komu je školení určeno:

Školení je určeno pro všechny pracovníky ve firmě, kteří pracují s počítačem, pohybují se na Internetu, pracují s firemními daty – manažeři na všech úrovních řízení, vedoucí pracovníci, obchodníci, asistentky, …

Hlavní cíle školení:

- Pochopit důležitost bezpečnosti při používání informačních a komunikačních technologií.
- Používat pro zabezpečení dat přístupová hesla a šifrovat soubory a daty nebo dokumenty tak, aby se k nim nedostali neoprávněné osoby.
- Umět se bezpečně pohybovat na Internetu.
- Umět ochránit počítač nebo mobilní zařízení před neoprávněným přístupem.
- Předcházet bezpečnostním problémům při komunikaci po Internetu při používání e-mailu, sociálních sítích a mobilních zařízeních.

Délka školení a místo konání:

1 den = 8 hodin

Výuka může být realizována v prostorách RHK Brno nebo v naší specializované učebně na některé z našich poboček.

Obsah školení:

- Princip bezpečnosti při práci s počítačem. Jak mohou být data v počítači ohrožena a jak je ochránit.

- Ukládání dat na externí úložiště (server, externí disk, USB flash disk, …). Rizika ukládání dat na internetová úložiště (Google Drive – freeware, Microsoft SkyDrive – freeware, Dropbox – freeware, uloz.to, uschovna.cz, …)
- Jak dodržovat zásady a pravidla bezpečnosti při používání informačních a komunikačních technologií.
- Zabezpečení pracovních a firemních souborů, složek a disků pomocí hesel, šifrování. Používání digitálního certifikátu.
- Ochrana počítače před škodlivými programy – malware, trojský kůň, rootkit, back door, … Používání antivirového programu.
- Jak bezpečně pracovat ve webovém prohlížeči (zjištění digitálního certifikátu webu apod.).
- Jak pracovat v počítačové síti tak, aby byla data ve firemním počítači vždy ochráněna. Používání firewallu na firemním počítači.
- Jak bezpečně pracovat v bezdrátové síti.
- Jak správně pracovat s elektronickou poštou – šifrování zpráv, používání digitálního podpisu elektronické pošty, rozeznat falešné zprávy nebo odkazy (phishing), …
- Bezpečné zálohování a likvidace dat.

Výukové materiály:

Každý účastník obdrží speciální výukové materiály odpovídající obsahu školení, cvičné příklady a testy.

Profil lektorů:

Výuku vedou certifikovaní lektoři IT – akreditovaní testeři ECDL, kteří mají mnohaletou praxi jak v daném oboru, tak ve vzdělávání dospělých.