Témata školení

Garant: Honza

Dát na PK web asap.

Jak si bezpečně přečíst potenciálně rizikový email

Anotace na web: Jak si bezpečně přečíst email, u něhož máte pochybnosti, zda vám nezaviruje počítač? Přišel vám podezřelý email, ale chcete si jej přečíst?

Znáte to. Přijde email. Vypadá divně. Člověk neví, jestli ho má rozkliknout. Když ho rovnou smaže, tak může přijít o zprávu, o kterou by přijít nechtěl. Ale když ho nesmaže a otevře ho, tak si možná zaviruje počítač. Co s tím?

Pro školitele - obsah školení:

- Podle čeho poznat podezřelý email?
- Vygooglit co se dá zjistit.
- Otevřít v privátním okně.
- Otevřít v odděleném účtu.
- Otevřít v JS-style virtuálu.
- Otevřít v JustSafe počítači od nás.
- Otevřít na ploše síťového stroje, který je k tomuto určený, refrešuje se.
- Otevřít ve virtuálním read-only stroji nabootovaném ze sítě.
- Nabootovat fyzický stroj virtuálně ze sítě.
- Podívat se na něj terminálem na Ux mailserveru.
- Velmi rizikové chování - mít na to dedikovaný počítač.
- Další mýty o bezpečném čtení mailů.
- Čemu dokáže zabránit a co nedokáže antivirák, antispyware a bezpečnostní záplaty?

Jak se bezpečně toulat webem

Anotace na web: Asi každý občas zabloudí na nějakou tu XXX stránku... Anebo na stránku s nelegálním obsahem. Jak si přitom nezavirovat počítač? A co když třeba škola vašeho dítěte (nebo třeba váš dodavatel) má zrovna zavirované stránky? Nebo prostě a jednoduše při brouzdání webem náhodou zabloudíte na nebezpečnou stránku a třeba o tom ani nevíte?

Pro školitele - obsah školení:

- Jak poznat podezřelou www stránku.
- Jaké riziko hrozí vašemu počítači, počítačům v sousedství, vašim datům, vaší práci.
- WHOIS, IP-locate
- Lynx style browsing
- Otevřít v privátním okně.
- Otevřít v odděleném účtu.
- Otevřít v JS-style virtuálu.
- Otevřít v JustSafe počítači od nás.
- Otevřít na ploše síťového stroje, který je k tomuto určený, refrešuje se.
- Otevřít ve virtuálním read-only stroji nabootovaném ze sítě.
- Nabootovat fyzický stroj virtuálně ze sítě.

- Antivirus proxy
- Velmi rizikové chování - mít na to dedikovaný počítač.
- Další mýty o bezpečném surfování
- Čemu dokáže zabránit a co nedokáže antivirák, antispyware a bezpečnostní záplaty?

Jak bezpečně používat homebanking a platit platebními kartami v eshopech

Anotace na web: Platíte platební kartou v eshopu nebo pracujete z mobilu nebo z počítače se svým bankovním účtem. Možná vás to už napadlo. Co když ta čísla, co tam klepu vidí i někdo další, nějaký hacker? Nebo co když eshopu někdo ukradne databázi zákazníků? A co když mám zavirovaný počítač nebo mobil? Seminář vysvětluje tato rizika a předvede možnosti jak je minimalizovat.

Pro školitele - obsah školení:

- Viry, spyware, hackeři
- Ukradená databáze
- Bezpečnost platební karty, co si lze v bance nastavit
- Bezpečnost internetbankingu, autorizační varianty
- PasswordKeyer device
- Otevřít v privátním okně.
- Otevřít v odděleném účtu.
- Otevřít v JS-style virtuálu.
- Otevřít v JustSafe počítači od nás.
- Otevřít na ploše síťového stroje, který je k tomuto určený, refrešuje se.
- Otevřít ve virtuálním read-only stroji nabootovaném ze sítě.
- Nabootovat fyzický stroj virtuálně ze sítě.
- Velmi rizikové chování - mít na to dedikovaný počítač.
- Další mýty o bezpečnosti karet a bankingu
- Čemu dokáže zabránit a co nedokáže antivirák, antispyware a bezpečnostní záplaty?

Cíle těchto školení

- Potkávat se s lidma, se studentama, IT a elektrikáři, vybírat si z nich staff, v obvyklém "kampusním stylu".
- Příjem ze vstupného, prodaných PK a SafeTerminálů.
- Najít buďto firmy nebo jednotlivce, které vyškolím, aby toto školili a nám z toho poběží pasivní příjem.

A ještě taky:

"Jak bezpečně posílat internetem soubory, aby se k jejich obsahu nikdo nedostal a aby nikdo cestou nepozměnil jejich obsah."