Jak předcházet možnému zneužití elektronické identity

Obecná doporučení pro přihlašování se do online služeb

Buďte informováni o přínosech a možných rizicích používání e-Identity, sledujte média.

Přemýšlejte, než kliknete na odkazy a bannery na webu nebo v emailu.

Před každým přihlášením na webové stránce zkontrolujte, jestli se viditelnáadresastránky shoduje s názvem, který obvykle používá daný poskytovatel.

Použití přihlašovacích prostředků: volba způsobu autentizace musí odpovídat pomyslné "hodnotě" Vaší personalizované transakce (platby a citlivé osobní údaje jen přes 2-faktorové přihlášení).

Používaná zařízení (počítače, tablety, mobily) a aplikace

Pravidelně aktualizujte své zařízení, jeho operační systém i aplikace.

Používejte aktualizované antivirové programy.

Nevyužívejte sdílené/veřejné počítače pro své personalizované transakce.

Nepoužívejte aplikace z neověřených zdrojů. Instalujte aplikace z webu důvěryhodných dodavatelů a ze softwarových tržišť (Google Play, Apple Appstore, Microsoft Store atd.).

Šifrujte úložiště vašich zařízení (tato funkce bývá součástí nebo nadstavbou operačního systému).

Nenechávejte svá zařízení bez dozoru. Zamykejte obrazovku při každém přerušení práce.

Při ztrátě jakéhokoliv zařízení nebo identitníhoprostředku si co nejdříve změňte související heslo nebo PIN.

Pro zabezpečení mobilních zařízení nepoužívejte gesta, ale buď biometriku (otisk prstu nebo rozpoznání obličeje) nebo PIN s minimální délkou 6 číslic.

Oddělujte svoje účty na zařízení od účtů dětí. Pro běžnou práci nepoužívejte účet s oprávněním administrátora.

Zvažte používání anti-tracking softwaru, který brání sledovacím technikám Vašeho chování na Internetu.

Používané sítě

Neprovádějte hodnotné transakce s přihlášením k e-Identitě přes veřejné pracovní stanice.

Pokud je to možné, nepracujte s e-Identitou přes nezabezpečené, nedůvěryhodné, nebo veřejné wifi sítě.

Musíte-li již pracovat s e-Identitou přes nedůvěryhodnou síť, použijte jako dodatečné opatření VPN (virtuální privátní síť). Zadůvěryhodnou síť lze považovat domácí wifi síť, wifi v zaměstnání, wifi u přátel s omezeným předáváním hesla, a dále mobilní sítěLTE a 5G.

Vypněte automatické přihlašování k uloženým wifi sítím, které považujete za nedůvěryhodné.

Webové stránky

Nenavštěvujte rizikové stránky a nespouštějte a neklikejte na soubory a odkazy, u nichž jednoznačně neznáte původ. Mějte na paměti, že pokud Vám určitá webová stránka nabízí zdarma něco, za co se jinde obvykle platí, je vyšší pravděpodobnost, že se Vám bude snažit implementovat malware (škodlivý kód).

Vyhýbejte se používání nezabezpečených webových stránek (http://,namísto správného https://), neboť tyto stránky nešifrují data při přenosu a neposkytují kontrolu skutečného majitele stránky - jeho certifikátu. Dále viz doporučení výše - kontrolujte, zda je na dané stránce aktivován protokol SSL/TLS a zda prohlížeč nehlásí podezřelou stránku.

Ověřte, že certifikát šifrovaného spojení TLS/SSL byl vydán pro subjekt (organizaci), která má poskytnout zamýšlenou službu.

Soubory a emaily

Neotvírejte soubory a nepovolujte makra, pokud si nejste jisti, že jsou od důvěryhodného odesílatele a neobsahují škodlivý kód.

Pozor na řetězové emaily, které mohou v příloze nést soubor se škodlivým kódem, neotevírejte přílohu.

Hesla a přihlašování prostřednictvím e-identity

Pro hodnotnější transakce pomocí e-identity preferujte takové prostředky pro přihlášení, které vůbec nepracují s klasickým heslem, nýbrž využívají zaregistrovaný fyzický druhý faktor (telefon, eOP, USB klíč apod.) odemykaný biometrikou nebo PINem. V takovém případě se přes Internet neposílá žádný statický (vždy stejný) řetězec, který může útočník lépe zachytit a následně zneužít.

Tam, kde prostředky e-identity pracují s klasickým heslem, používejte silná hesla (se zapojením velkých a malých písmen, číslic a zvláštních znaků) nebo dlouhá / frázová hesla. Tato hesla nepoužívejtepro žádné jiné účty nebo virtuální identity, a pokud si je zapíšete, tak jedině doma "do trezoru" nebo do speciální, k tomu určené, aplikace, viz níže.

e-identita
****

Nikdy a nikomu nedávejte své přihlašovací údaje a neumožňujte přístup a PIN k druhému ověřovacímu prostředku (telefon, eOP, USB klíč apod.)

Využívejte dva nebo více různých prostředků e-Identity - nejlépe jeden s úrovní záruky "značná" a jeden s úrovní "vysoká", abyste měli alternativu v případě problémů s jedním prostředkem.Pokud si nejste schopni všechna svá hesla zapamatovat, využívejte ověřené správce hesel.

Hesla a ověřování

Pokud si nejste schopni všechna svá hesla zapamatovat, využívejte ověřené správce hesel.

Využívejte více faktorovou autentizaci.

Kontrolujte autenticitu webové stránky, kam zadáváte svá hesla.

Nezadávejte hesla na cizích zařízeních.

Neukládejte hesla do paměti prohlížeče, pokud prohlížeč neobsahuje šifrování vlastním heslem.

****

e-identita