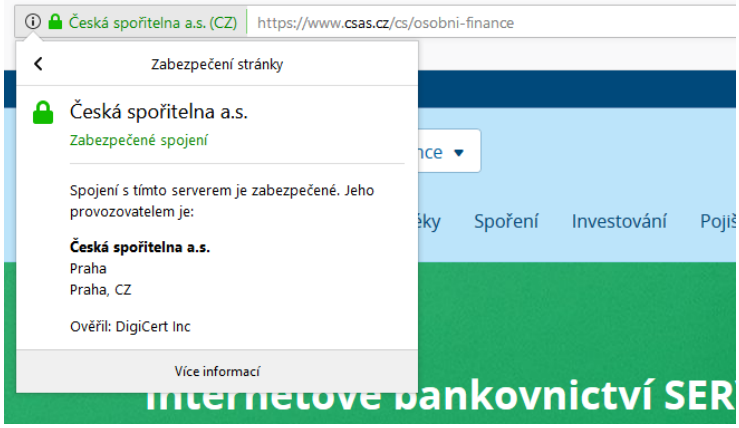
SPCSS
Státní pokladna
Centrum sdílených služeb

Doporučení pro bezpečné platby a nakupování online

Platební karty a internetové bankovnictví

1. Nesdělujte nikomu přihlašovací údaje k internetovému bankovnictví, a to ani nejbližším rodinným příslušníkům. Své přihlašovací údaje do internetového bankovnictví nikdy neukládejte do paměti v prohlížeči.
2. Nepřihlašujte se k elektronickému bankovnictví na veřejném počítači, který může obsahovat škodlivý software schopný zkopírovat vaše přihlašovací údaje.
3. Vždy, když je to možné, používejte vícefaktorovou autentizaci.
4. Aktualizujte si svůj osobní počítač, používejte antivirovou kontrolu a firewall.
5. Na běžném účtu nedržte vetší obnos peněz, vyšší částky by mely být uloženy na spořicím nebo jiném účtu, tedy mimo dostupnost pro platbu kartou.
6. Stanovte si denní limit pro maximální výši peněžní transakce zadané přes internetové bankovnictví a pro výběr z bankomatu. Kontrolujte si pravidelně stav svého účtu, historii přihlášení a provedené transakce.
7. Pořiďte si platební kartu, kterou budete používat výhradně pro platby přes internet – tu pak nechávejte doma a s sebou pro placení nákupů v obchodech noste kartu, která bude mít zablokované platby po internetu. Některé banky nabízejí pro platby přes internet možnost zřízení virtuální platební karty (fyzicky neexistuje, jedná se pouze o 16místné číslo se stanoveným datem platnosti a kontrolním kódem CVC nebo CVC2).
8. Pamatujte, že banka nikdy neoslovuje klienty e-mailem a nežádá pomocí něj o zaslání jakýchkoliv osobních dat, přihlašovacích údajů, hesel, PINů, atd.

9. Vždy se ujistěte o správnosti adresy v adresním řádku (klikněte na zámeček), např. Česká spořitelna má oficiální stránky www.csas.cz, objevily se již podvodné phishingové stránky www.ceskasporitelna.cz. Kontrolujte také přítomnost HTTPS certifikátu.



10. Když už jsme u phishingu, v předvánoční době se pravidelně objevují nové způsoby podvodného jednání. V loňském roce se jednalo o sms zprávy z „Alzy", které nabízely nákup zdarma po stažení určité aplikace. Alza se stala terčem podobného útoku i později, tyto sms informovali o doručení balíčku a o možnosti vyhrát iPhone X za 1 korunu. Na tyto zprávy nereagujte a neklikejte na případný odkaz.
11. Vyhýbejte se nezabezpečeným a neznámým Wifi sítím, nikdy se přes ně nepřihlašujte do internetového bankovnictví, e-mailu ani jinam, kde mohou být odposlechnuty vaše přístupové údaje.