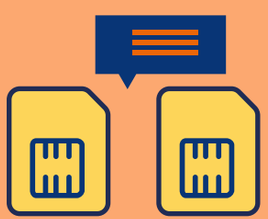
SIM SWAPPING (OVLÁDNUTÍ MOBILNÍHO TELEFONNÍHO ČÍSLA) – PODVOD PROSTŘEDNICTVÍM MOBILNÍHO TELEFONU

SIM Swapping nastane, když podvodník převezme pomocí technik sociálního inženýrství kontrolu nad vaší SIM kartou prostřednictvím vašich ukradených osobních údajů.

JAK TO FUNGUJE?

Podvodník získává osobní údaje oběti např. prostřednictvím úniku dat, phishingu, vyhledávání na sociálních sítích, škodlivých aplikací, nakupování na internetu, malwaru atd.

S těmito informacemi podvodník oklame mobilního operátora a nechá převést číslo mobilního telefonu oběti na SIM, kterou vlastní.



Podvodník nyní může přijímat příchozí hovory a textové zprávy a má přístup do internetového bankovnictví oběti.

Oběť si všimne ztráty přístupu k mobilním sítím a nakonec zjistí, že se nemůže přihlásit ke svému bankovnímu účtu.

JAK SE BRÁNIT?

- Mějte aktualizovaný software, včetně prohlížeče, antiviru a operačního systému.
- Omezte osobní informace na sociálních sítích a chovejte se obezřetně.
- Nikdy neotvírejte podezřelé odkazy nebo přílohy, které dostanete e-mailem nebo textovou zprávou.
- Neodpovídejte na podezřelé e-maily ani nejednejte s volajícími, kteří požadují vaše osobní údaje.
- Pravidelně aktualizujte svá hesla.
- Stahujte aplikace pouze od oficiálních poskytovatelů a vždy si přečtěte oprávnění požadovaná aplikacemi.
- Pokud je to možné, nespojujte své telefonní číslo s citlivými online účty.
- Nastavte si vlastní PIN pro přístup k SIM kartě. Tento PIN nikomu nesdělujte.
- Často kontrolujte své finanční výpisy.

JSTE OBĚŤ?

- Pokud váš mobilní telefon bezdůvodně ztratí příjem, okamžitě to nahlaste svému poskytovateli služeb.
- Pokud poskytovatel služby potvrdí, že byla vaše SIM karta ovládnuta někým jiným, nahlaste to policii.

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
ČBA ČESKÁ BANKOVNÍ ASOCIACE | CZECH BANKING ASSOCIATION
POLICIE ČESKÉ REPUBLIKY

#CyberScams