WEBOVÉ HROZBY

DVAKRÁT SE PODÍVEJTE, NEŽ KLIKNETE

Mohli byste přijít o peníze, své osobní informace nebo dokonce o svá uložená data, když vaše zařízení přestane fungovat. Nenechejte se nachytat!

JAK K TOMU MŮŽE DOJÍT?

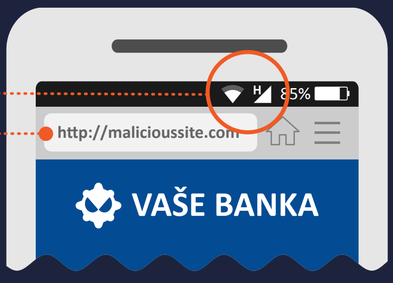
PHISHINGOVÉ ÚTOKY: Nalákají uživatele k poskytnutí osobních informací tím, že se vydávají za důvěryhodnou organizaci. Šíří se e-mailem, textovou zprávou nebo přes sociální média.

PROHLÍŽENÍ WEBOVÝCH STRÁNEK: Vaše mobilní zařízení může být napadeno při pouhé návštěvě nebezpečné stránky.

STAHOVÁNÍ SOUBORŮ: Škodlivé odkazy a přílohy mohou být součástí e-mailu.

PROČ TO FUNGUJE?

Mobilní zařízení jsou cNEUSTÁLE PŘIPOJENÁ k internetu.



Obecným problémem je OMEZENÁ PLOCHA OBRAZOVKY. Uživatelé mobilních zařízení zobrazují adresy URL na malé ploše. To znamená, že je obtížné vidět, zda je doména legitimní.

DŮVĚRA UŽIVATELE v osobní charakter mobilního zařízení.

CO MŮŽETE DĚLAT?

Mějte se na pozoru, pokud obdržíte SMS nebo hovor od společnosti žádající vaše osobní informace. Takovou zprávu nebo hovor můžete ověřit, když zavoláte na oficiální číslo společnosti.

Při prohlížení webu na vašem mobilním zařízení se ujistěte, že je vaše připojení zabezpečené přes HTTPS. Můžete to vždy zkontrolovat na začátku adresy URL.

Nikdy neklikejte na odkaz/přílohu v nevyžádaném e-mailu nebo SMS. Okamžitě takovou zprávu smažte.

Buďte obezřetní, pokud se dostanete na stránku s řadou gramatických chyb překlepů nebo na stránku s nízkým rozlišením.

Pokud je to možné, nainstalujte si aplikaci pro zabezpečení mobilního zařízení, která vás upozorní na jakoukoli podezřelou aktivitu.

EUROPOL EC3 European Cybercrime Centre | POLICIE ČESKÉ REPUBLIKY | NCBI #NárodníCentrumBezpečnějšíhoInternetu | saferinternet.cz

#MobileMalware