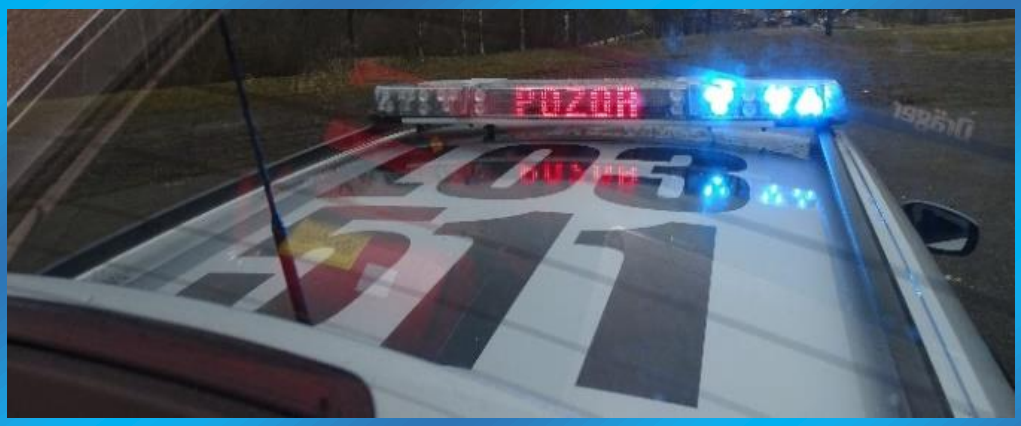
VAROVÁNÍ !!!

PODVODNÍCI VYKRÁDAJÍ BANKOVNÍ ÚČTY

Policie ČR varuje širokou veřejnost před podvodným jednáním pachatelů trestné činnosti, kteří zcizují finanční prostředky z bankovních účtů osob.



- **Podvodníci se vydávají za zaměstnance bank či dokonce policisty.**
- **Pachatelé telefonují klientům bank s legendou, že byl napaden jejich účet.**
- **Následně vmanipulují osobu buď k převedení finančních prostředků na jiný účet nebo vložení peněz do bitcoinového automatu nebo ke sdělení informací pro vstup do internetového bankovnictví.**
- **Podvodníci také využívají vzdálený přístup do počítače poškozených.**
- **Pod záminkou pomoci přesvědčí klienta banky k instalaci programů AnyDesk a TeamViewer, tyto programy umožňují pachatelům přístup do daného PC.**
- **Pro důvěryhodnost podvodníci sdělí volané osobě, že se případem napadení účtu již zabývá kriminální policie a že ji bude v následujícím telefonátu kontaktovat policista.**
- **Vzápětí skutečně telefonuje „podvodný policista“, aby podpořil smyšlený příběh.**
- **K podpoření věrohodnosti legendy pachatelé využívají reálná jména i reálné útvary a dokonce i reálná telefonní čísla bank nebo Policie ČR.**
- **Vše působí velice profesionálně.**

UPOZORŇUJEME !!!

- **Žádná banka se svými klienty nikdy nejedná tímto způsobem.**
- **Nikdy po klientovi nemůže chtít přístupové údaje k bankovním účtům, hesla, PIN kódy.**
- **To vše jsou údaje, které se nikomu nesdělují, a to ani v této době, kdy se kvůli pandemii omezují osobní kontakty a komunikace probíhá telefonicky či psanou formou.**

Preventivní rady, jak se zachovat:

- **Nereagujte na podobné hovory, SMS zprávy, e-maily, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení.**
- **V žádném případě nesdělujte k Vaší osobě žádné citlivé údaje ani bezpečností údaje z vaší platební karty, nebo přístupové údaje k online bankovnictví.**
- **Nikdy nikomu nesdělujte a ani nepřeposílejte bezpečnostní / autorizační kód, který Vám přišel formou SMS zprávy.**
- **Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.**
- **Nikdy nikomu podezřelému neumožňujte vzdálený přístup do Vašeho počítače.**
- **Sledujte a pečlivě čtěte informace od Vaší banky v internetovém bankovnictví.**
- **Při každém vstupu do internetového bankovnictví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje.**
- **Aktualizujte software, antivirový program, firewall.**
- **Během, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které Vám útočník sdělil (jména, e-mailové adresy, čísla účtů, odkazy na webové stránky, apod.)**

Pokud se vám již skutečně něco podobného stalo nebo stane, věc bezprostředně oznamte na Policie ČR prostřednictvím bezplatné tísňové linky 158 nebo na kterékoliv policejní služebně a informujete svůj bankovní ústav.