INFORMACE O ČLENSTVÍ

Máte-li pocit, že činnost Sdružení obrany spotřebitelů – Asociace, z.s. je prospěšná, staňte se naším členem.
O výši svého členského příspěvku si rozhodnete sami.

VÝHODY ČLENSTVÍ

- získáte pravidelné informace o novinkách a nástrahách ve spotřebitelském prostředí,
- budeme Vás zvát na naše akce, besedy a veřejná vystoupení,
- budete přednostně odbaveni v naší elektronické poradně (možno podávat dotazy přes elektronický formulář),
- budete si moci objednat konkrétní čas v našich 10 osobních poradnách, které v takto velké šíři poskytujeme jako jediní v ČR
- přednostně odbaveni v našich 10 osobních poradnách
- budeme Vám zasílat náš magazín SOSák a pravidelné NEWSlettery,
- poskytneme Vám nadstandardní poradenství, poskytneme Vám vzorové dopisy a pomůžeme Vám při jejich sepsání,
- dostanete členskou kartu, se kterou u nás můžete čerpat veškeré výhody,
- podpoříte naši činnost do budoucna.

JAK SE STÁT ČLENEM

Možnost přispívat občasně i pravidelně jakoukoliv částkou dle Vašich možností

1) OSOBNĚ
– na kterékoliv naší poradně nebo v našem centru na adrese Česká 141/31, 602 00 Brno

2) ELEKTRONICKY
- www.asociace-sos.cz/clenstvi/

3) BANKOVNÍM PŘEVODEM
- členský příspěvek můžete zaslat také převodem na číslo účtu 2600115708/2010, jako variabilní číslo uveďte datum narození v úpravě podle tohoto vzoru
– např. pro datum narození 6. 4. 1951 je variabilní symbol 510406
- informujte nás prosím emailem clenove@asociace-sos.cz o úhradě členského příspěvku, ať můžeme ještě před obdržením platby připravit Vaši členskou kartičku. Do předmětu zprávy uveďte „členský příspěvek"

Máte-li zájem o členství v naší organizaci, kontaktujte nás prosím na e-mail: clenove@asociace-sos.cz nebo telefonicky 771 191 191

SOS ASOCIACE
SDRUŽENÍ OBRANY SPOTŘEBITELŮ

KDE NÁS NAJDETE:
SOS – Asociace, z. s.
Česká 141/31, 602 00 Brno

PORADENSTVÍ
po – pá 9.00 - 16.00
+420 771 191 191
Whatsapp poradenství
poradna@asociace-sos.cz
www.asociace-sos.cz

Sledujte nás

Pomohla Vám naše činnost, myslíte si, že je naše činnost prospěšná? Staňte se naším sympatizujícím členem a můžete nám přispívat občasně či pravidelně jakoukoliv částkou dle Vašich možností.

Číslo bankovního účtu
2600115708/2010

Děkujeme...

Pomáhají nám:

MINISTERSTVO PRŮMYSLU A OBCHODU
BRNO
PRAHA PRAGUE PRAGA
Jihočeský kraj
tábor
PROSTĚJOV
Vyškov
OZ ADVOKÁTNÍ KANCELÁŘ JUDr. Ondřej Zelenka
SPOTŘEBITELSKÉ FÓRUM
K&P PARTNERS ADVOKÁTNÍ KANCELÁŘ

www.asociace-sos.cz

TRVEJTE NA SVÝCH PRÁVECH

Bankovní PODVODY



SOS ASOCIACE
SDRUŽENÍ OBRANY SPOTŘEBITELŮ

Finanční a bankovní PODVODY

Finanční a bankovní podvody jsou protiprávní jednání, při nichž pachatelé zneužívají finanční operace, majetek nebo důvěrné údaje s cílem obohatit se na úkor jiných. Tyto praktiky mají mnoho forem – my Vám přinášíme přehled těch nejčastějších.

DRUHY FINANČNÍCH A BANKOVNÍCH PODVODŮ

Podvody s kreditními kartami

- **Phishing:** Podvodníci se snaží získat údaje, jako jsou čísla kreditních karet, prostřednictvím falešných e-mailů nebo webových stránek.
- **Skimming:** Zařízení na bankomatech nebo platebních terminálech, které kopíruje informace z kreditních karet.

Podvody s investicemi

- **Ponziho schéma:** Podvodníci lákají nové investory na vysoké výnosy z vkladu, přičemž výnosy pro starší investory se platí z vkladů nových investorů, dokud tento systém nezkrachuje.
- **Pump and dump:** Podvodníci uměle navyšují ceny akcií, aby ji následně prodali za vysokou cenu, zatímco ostatní investoři na to doplatí.

Podvody s hypotékami

- **Falešné hypoteční poradenství:** Podvodníci se vydávají za odborníky na hypoteční poradenství, vybírají poplatky, ale neposkytují reálné služby.

Podvody v online bankovnictví

- **Malware a Ransomware:** Podvodníci prostřednictvím škodlivého softwaru (malware) získají přístup k účtu oběti
- **Vishing:** Telefonní podvody, při nichž se podvodníci vydávají za falešné zástupce bank s cílem získat přihlašovací údaje.

JAK SE VYHNOUT FINANČNÍM A BANKOVNÍM PODVODŮM?

Bránit se finančním podvodům je klíčové pro ochranu vašich peněz a osobních údajů. Podvodníci se stále vyvíjejí a přicházejí se stále sofistikovanějšími metodami, jak obelstít jednotlivce nebo firmy, ale existuje několik zásadních kroků, kterými můžete riziko minimalizovat.

Buďte ostražití a skeptičtí vůči příliš výhodným nabídkám

- **Neuvěřitelně vysoké sliby:** Nabídka neuvěřitelně vysokých výnosů nebo příliš výhodných nabídek, je často signálem podvodu.
- **Vyhněte se tlaku:** Pokud na vás prodejce naléhá k okamžitému rozhodnutí (např. nabídka, která platí jen dnes), buďte obezřetní. Podvodníci často používají nátlak k tomu, aby vás přiměli k rozhodnutí bez rozmyšlení.

Ověřujte nabídky a společnosti

- **Prověřte legitimitu:** Pokud obdržíte nabídku na investice, půjčky nebo produkty, firmu si prověřte (např. prostřednictvím obchodního rejstříku, recenzí).
- **Falešné webové stránky:** Zkontrolujte URL adresu a doménu webových stránek, podvodníci používají domény, které se jen lehce liší od těch oficiálních (např.: „.com“ místo „.cz“).
- **Sociální sítě a recenze:** Zkontrolujte si, jestli má firma na sociálních sítích aktivní profil. Pokud firma neexistuje online nebo nemá žádné pozitivní recenze, je lepší se jí vyhnout.

Nikdy neklikejte na podezřelé odkazy nebo přílohy

- **Phishing:** Své citlivé údaje nesdělujte nikkomu přes e-mail ani přes telefon, pokud si nejste jisti, že komunikujete s legitimní osobou. Nikdy neklikejte na odkazy v nevyžádaných e-mailech.
- **Kontrolujte URL adresy:** Ujistěte se, že webové stránky jsou správně zabezpečeny (https://) a že jsou autentické.
- **Přílohy:** Buďte opatrní při otevírání příloh nebo stahování souborů z neznámých e-mailů nebo zpráv.

Používejte silná a unikátní hesla

- **Bezpečné heslo:** Používejte složitá hesla, která obsahují kombinaci písmen, číslic a speciálních znaků. Vytvořte si různá hesla k jednotlivým online účtům. Nevytvářejte jednoduchá hesla jako „123456“ nebo „password“.
- **Dvoufaktorová autentizace:** Aktivujte dvoufaktorovou autentizaci (2FA) tam, kde je to možné, zejména na bankovních účtech a důležitých online službách. To zajišťuje, že k vašim účtům mají přístup pouze oprávněné osoby.

Monitorujte pravidelně své účty

- **Kontrola transakcí:** Pravidelně kontrolujte výpisy z banky a kreditních karet, abyste zjistili jakékoli neautorizované transakce. V případě, že zjistíte něco podezřelého podezřelého, kontaktujte banku.
- **Upozornění na transakce:** Většina bank nabízí upozornění na podezřelé transakce nebo platby. Aktivujte tuto službu, abyste byli včas informováni o jakýchkoli změnách.

Zabezpečte své zařízení

- **Antivirus a firewall:** Ujistěte se, že vaše zařízení má anti virový software a zapnutý firewall.
- **Aktualizace:** Pravidelně aktualizujte operační systém a software na vašem zařízení.
- **Zabezpečení Wi-Fi:** Ujistěte se, že vaše Wi-Fi je chráněna silným heslem a používá šifrování (např. WPA2 nebo WPA3).

Neposílejte peníze na neznámé účty

- **Platba prostřednictvím gift cards nebo kryptoměn:** Pokud po vás někdo požaduje platbu prostřednictvím gift cards nebo kryptoměn (např. Bitcoin), buďte opatrní – podvodníci tuto formu platby často využívají.

JAK REAGOVAT, KDYŽ SE STANETE OBĚTÍ PODVODU?

- **Okamžitě kontaktujte svou banku:** Pokud zjistíte, že vám z účtu zmizely peníze, okamžitě kontaktujte svou banku.
- **Změňte si hesla a zabezpečte účty:** Pokud došlo k úniku citlivých údajů, změňte si přístupové údaje k účtům (e-mail, bankovní účty, sociální sítě).
- **Nahlaste podvod:** Nahlaste podvod na Policii ČR, v případě bankovního podvodu se můžete také obrátit na Finančního arbitra.

Potřebuje poradit i s jiným problémem?