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:

KANCELÁŘ

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

www.asociace-sos.cz

TRVEJTE NA SVÝCH PRÁVECH

Jak poznat PODVODNÉ PRAKTIKY a jak se proti nim bránit



SOS ASOCIACE
SDRUŽENÍ OBRANY SPOTŘEBITELŮ

Jak poznat PODVODNÉ PRAKTIKY a jak se proti nim bránit

S rozvojem technologií sdílíme na internetu stále více informací – od e-mailu, přes fotky až po čísla platebních karet. Neopatrnost ale může vést k zneužití našich dat, ztrátě soukromí či finančním škodám, a proto je důležité vědět, jak tyto údaje chránit.

JAK POZNAT PODVODNÉ PRAKTIKY?

Podvodníci přicházejí se stále sofistikovanějšími podvody a jejich **nabídky mohou působit velmi důvěryhodně**.

Hlavní znaky a rady, jak se bránit:

Neuvěřitelné nabídky nebo sliby

- Podvodníci často slibují nereálné výhody (například extrémně vysoké výnosy z investic) nebo rychlé zbohatnutí.

Příklad: *Podvodné investiční nabídky, kde vám někdo slibuje návratnost několika tisíc procent ročně, což je obvykle nerealistické.*

Nátlak na rychlé rozhodnutí

- Urgentní a naléhavé požadavky jsou často známkou podvodu. Podvodníci vás mohou tlačit do rychlého rozhodování pod záminkou, že nabídka „trvá pouze dnes“, nebo že máte jen omezený čas na zajištění výhodné nabídky.

Příklad: *E-maily nebo telefonáty, které vás nutí k okamžitému převodu peněz nebo k poskytnutí osobních údajů.*

Neověřené kontakty nebo neznámé osoby

- Podvodníci se často vydávají za známé instituce, firmy nebo osoby, ale mohou mít špatně napsané názvy, podezřelé e-mailové adresy nebo telefonní čísla.

Příklad: *E-maily, které vypadají, jako by byly z vaší banky, ale obsahují chyby v jazyce nebo neznámé kontaktní údaje.*

Požadavky na osobní a citlivé údaje

- Nikdy nesdělujte své osobní a citlivé údaje (jako číslo účtu, přihlašovací údaje, číslo kreditní karty) bez důkladné verifikace, že daný požadavek je legitimní. Banky ani jiné instituce po vás tyto údaje nikdy nebudou chtít.

Příklad: *Požadavek na zaslání přihlašovacích údajů k online bankovnictví prostřednictvím e-mailu nebo SMS zprávy.*

Neznámé nebo nesprávně fungující webové stránky

- Podvodné webové stránky mohou mít chybějící kontaktní informace nebo podezřelou grafiku

Příklad: *Webová stránka s nabídkou výhodného zboží neobsahuje žádné kontaktní informace nebo obchodní podmínky.*

Podivné platební metody

- Požadavek na platbu prostřednictvím neověřených metod, jako je kryptoměna, převody přes neoficiální platformy (např. Western Union) nebo platby na neznámé účty.

Příklad: *Případ, kdy vás někdo požádá, abyste zaplatili za zboží či službu přes neověřenou platební platformu, která není podporována známými finančními institucemi.*

Gramatické chyby a špatný jazyk

- Podvodné e-maily často obsahují gramatické chyby, nesmyslné formulace nebo zvláštní styl psaní, který je odlišný stylu komunikace s oficiálními institucemi.

Příklad: *E-mail od „vaší banky“, který obsahuje chyby v textu.*

JAK SE BRÁNIT PROTI PODVODNÝM PRAKTIKÁM?

Buďte skeptičtí vůči nečekaným nabídkám

- Pokud dostanete nevyžádaný e-mail, telefonát nebo zprávu s nabídkou, která vám připadá podezřelá nebo neuvěřitelná, zkontrolujte její legitimitu.

Tip: Neposkytujte osobní údaje, pokud nevíte, kdo se ptá. Ověřte si informace přímo u dané instituce.

Neposílejte peníze neznámým osobám

- Nikdy nezasílejte peníze, gift cards, nebo kryptoměny nikomu, u koho si nejste jisti jeho identitou. Ověřené společnosti nebo osoby nikdy nepožadují platby touto formou.

Tip: Pokud vám přijde e-mail s tím. že jste vyhráli peníze nebo jinou výhru, ale musíte zaplatit „poplatek“ nebo „daně“ před tím, než vám bude výhra vyplacena, jedná se o podvod.

Používejte silné a jedinečná hesla

- Pro přístup k vašim bankovním účtům, online účtům, anebo e-mailu použijte silná a jedinečná hesla.

Kontrolujte webové adresy (URL)

- Před kliknutím na odkaz v e-mailu zkontrolujte, zda adresa začíná „https://“ (což znamená šifrování) a jestli je název domény správný. Podvodníci často používají domény, které vypadají podobně, ale mají jemné rozdíly (např. rozdílnou koncovku „.com“ místo „.cz“).

Pravidelně monitorujte účty

- Pravidelně kontrolujte své bankovní výpisy, elektronické bankovnictví. Pokud zjistíte nějakou podezřelou transakci nebo něco neobvyklého, neprodleně kontaktujte svou banku.

Ověřujte telefonáty a e-maily

- Pokud obdržíte podezřelý telefonát nebo e-mail od nějaké společnosti (např. vaší banky), zavolejte zpět na oficiální telefonní číslo, které najdete na jejich webových stránkách, a ověřte si informace.
- Pamatujte: Banka nikdy nebude chtít vaše heslo ani PIN.

Zabezpečte své zařízení

- Aktualizujte software a antivirus na svých zařízeních, abyste se chránili před malwarem a phishingovými útoky.

Tip: Nikdy neklikejte na odkazy nebo přílohy z neznámých e-mailů nebo zpráv.

Vzdělávejte se v oblasti podvodů

Zůstaňte informovaní o nejnovějších typech podvodů. Některé banky či jiné finanční instituce pravidelně zveřejňují varování a informace o aktuálních podvodných praktikách.

CO DĚLAT, KDYŽ SE STANETE OBĚTÍ PODVODU?

- Okamžitě kontaktujte svoji banku a informujte ji o podezřelé transakci.
- Změňte hesla na všechny online účty které mohou být ohroženy.
- Nahlaste podvod příslušným orgánům (Policie ČR, Finanční arbitr).

Potřebuje poradit i s jiným problémem?