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...

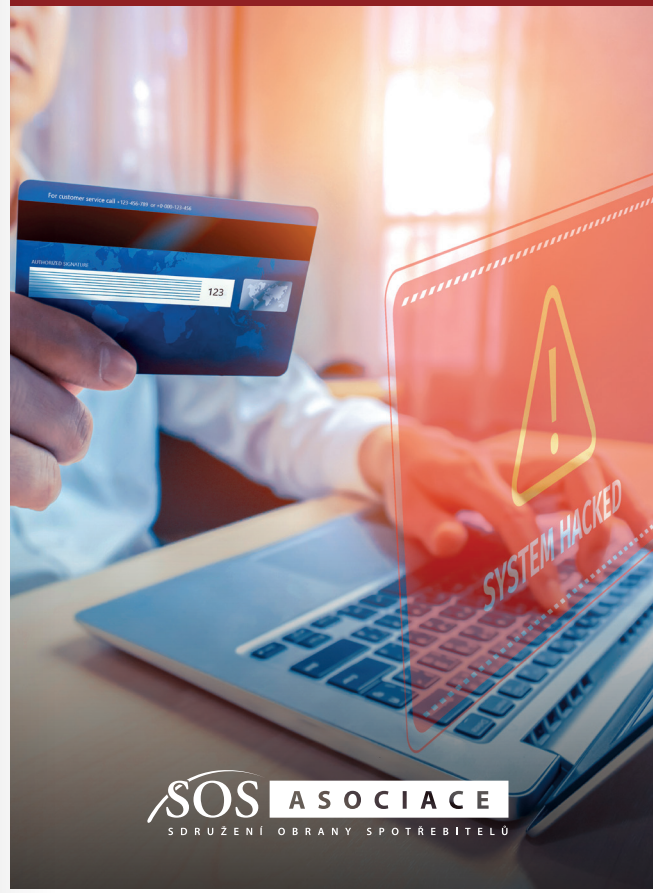
Pomáhají nám:

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

Internetové PODVODY



Internetové PODVODY

Rozpoznání podvodů na internetu může být náročné, protože podvodníci se stále více zdokonalují ve vytváření autentických a důvěryhodných situací. My vám ale představíme několik klíčových znaků internetových poidvodů, které vám mohou pomoci odhalit podvod a efektivně se proti němu bránit.

PHISHING

Phishing (česky se často říká „**phishingový útok**“) je **forma internetového podvodu**, při které se útočník vydává za důvěryhodnou osobu nebo instituci (např. banku, dopravní službu, úřad, e-shop).

Cíl phishingu:
- vylákat od tebe citlivé údaje – hesla, čísla platebních karet, přístup do internetového bankovnictví, nebo osobní informace.

Jak phishing vypadá:
- přijde ti e-mail nebo SMS, která vypadá „oficiálně“, ale je falešná,
- zpráva tě často nutí kliknout na odkaz a rychle jednat (např. zaplatit poplatek, přihlásit se, potvrdit údaje),
- odkaz vede na podvodnou stránku, která napodobuje skutečný web (např. banky).

Příklad phishingu:
„Váš účet byl zablokován. Přihlaste se ihned a potvrďte své údaje na odkazu níže.“

Jak se chránit:
- nikdy neklikej na podezřelé odkazy v e-mailech nebo SMS,
- vždy si ověř adresu webu (musí být správně napsaná a začínat https://),
- pamatuj, že banka nebo úřad nikdy nežádá zaslání hesla e-mailem nebo SMS.

PODVODNÉ E-SHOPY

Podvodný e-shop je internetový obchod, který vypadá na první pohled jako běžný, ale jeho cílem je vylákat peníze od zákazníků bez dodání zboží (nebo pošle padělky/nekvalitní výrobky).

JAK PODVODNÝ E-SHOP POZNÁŠ:

- ceny jsou podezřele nízké (např. značkové boty za třetinu běžné ceny),
- chybí kontaktní údaje – adresa, IČO, telefon,
- web má jen e-mailovou schránku typu „@gmail.com“ nebo „@seznam.cz“,
- často chybí obchodní podmínky nebo jsou zkopírované z jiných stránek,
- platba je možná jen předem kartou nebo převodem, neexistuje dobírka,
- doména (adresa webu) je často nově registrovaná, někdy s podezřelým názvem.

JAK SE CHRÁNIT:

- nakupuj jen v ověřených e-shopech (recenze, známá značka, historie),
- zkontroluj, zda má obchod platné IČO a skutečný kontakt,
- hledej recenze na nezávislých stránkách (nejen na webu e-shopu),
- pokud cena zní „až příliš dobře, aby to byla pravda“, je to nejspíš podvod.

INVESTIČNÍ PODVODY

Investiční podvod je typ internetového (nebo telefonického) podvodu, při kterém podvodníci slibují rychlý a vysoký zisk bez rizika, aby vylákali peníze od lidí.

Jak vypadá investiční podvod:
- reklamy na sociálních sítích s tvářemi celebrit (falešně) – „I já jsem vydělal miliony na kryptoměnách!“
- telefonát od „poradce“ nebo „makléře“, který nabízí „jedinečnou příležitost“ k investici,
- slibují jistotu výnosu (např. 200 % za měsíc) – což v reálných investicích neexistuje,
- požadují, abys rychle poslal peníze (často na zahraniční účet),
- po prvním vkladu tě lákají vložit více („vidíte, už vyděláváte, pošlete další částku“),
- nakonec peníze zmizí a kontakt přestane fungovat.

JAK SE CHRÁNIT:

- nevěř slibům snadného a rychlého zisku,
- ověř si, zda má firma licenci u České národní banky (CNB),
- nikdy neposílej peníze na neznámé účty a nenechávej si nainstalovat programy pro vzdálený přístup (TeamVie-wer, AnyDesk) – podvodníci je často zneužívají.

VIRY A MALWARE

Viry a malware jsou škodlivé programy, které se šíří přes internet a mohou poškodit tvůj počítač, mobil nebo ukrást tvoje data.

CO TO JE:

- Viry – malé programy, které se připojí k souborům a šíří se dál (např. e-mailem).
- Malware – obecný pojem pro škodlivý software (viry, trojské koně, spyware, ransomware).
- Ransomware – zablokuje soubory a požaduje vý-kupné.
- Spyware – tajně sleduje tvoji činnost a krade hesla.
- Trojský kůň – tváří se jako neškodná aplikace, ale škodí „zevnitř“.

JAK SE ŠÍŘÍ:

- přes přílohy v e-mailech,
- podvodné odkazy na webu,
- pirátské programy a hry,
- nakažené USB disky.

JAK SE CHRÁNIT:

- nikdy neotvírej podezřelé přílohy a odkazy,
- používej antivirový program a firewall,
- pravidelně aktualizuj software i operační systém,
- stahuj jen z oficiálních obchodů (Google Play, App Store).

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?