Redamp.io

WEBINÁŘ PRO ŽIVNOSTNÍKY A MALÉ FIRMY

Kybernetický incident. Co dělat?

První kroky, koho kontaktovat, co nedělat a jak omezit další škody.



ING. DOMINIK MALČÍK, PH.D. · REDAMP.IO · LISTOPAD 2026

pro podnikavé

PODLE POLICIE ČR

Čtyři věci.
Na žádnou nezapomeňte.

Klid

OVĚŘUJTE

Zavěste a ověřte. Podvodník sází na spěch.

Obrana

ZASTAVTE ŠKODU

Banka, odpojení od sítě / vypnutí, nová hesla.

Pomůže vám IT technik.

Důkazy

UCHOVEJTE DŮKAZY

Nic nemažte. Uložte zprávy a výpisy.

Komunikace

OZVĚTE SE

Banka, IT technik, policie, pojišťovna, zákazníci a obchodní partneři.

⚠ **Nejsou to kroky po sobě, často běží současně. Vždy ale platí: nejdřív zamezte dalším škodám.**

V roce 2025 registrovala Policie ČR 21 137 skutků v kyberprostoru, v průměru 58 denně.

KLID

Spěch je zbraň podvodníka.

Jak poznáte podvodný hovor:

- Volá „banka“ nebo „policie“ a tlačí na čas.
- Chce převod na „bezpečný účet“ nebo instalaci aplikace.
- Chce hesla nebo kódy z SMS.

Policie radí: „Zastav. Zavěs. Zkontroluj.“ Bance volejte sami na oficiální číslo z karty, aplikace nebo webu.



ILUSTRAČNÍ PŘÍKLAD

Podvržené číslo

Na displeji může být i pravé číslo banky.

Tlak na čas

Má vám zabránit v přemýšlení.

Bezpečný účet

Banka ani policie ho po vás nikdy nechtějí.

OBRANA

Nejdřív zastavte škodu.
Pak měňte hesla.

PENÍZE

Volejte banku

Prozradili jste přístupy nebo údaje z karty, potvrdili podezřelou platbu, odešly peníze? Řekněte bance, co se stalo, a požádejte o blokaci ohrožené karty nebo přístupu.

POČÍTAČ

Odpojte od sítě

Odpojte kabel, vypněte Wi-Fi a volejte IT technika.

Nejde odpojit? Pak ho vypněte.

UŽIVATELSKÉ ÚČTY

Změňte hesla

Z jiného, nezasaženého zařízení. Nejdřív e-mail, přes něj jde obnovit hesla jinde. Pak dvoufázové ověření.

Při napadení počítač sami nečistěte. Domluvte se s IT technikem.

DŮKAZY

Nemažte.
Uložte.

Smazaná zpráva je ztracená stopa pro banku, pojišťovnu i policii.

Co si uložit:

- Snímek zprávy a adresu podvodného webu.
- Výpis z účtu s podezřelou platbou.
- Na papír: kdy, co jste udělali, s kým.

Zprávu už jste smazali? Incident nahlaste i tak.



ILUSTRAČNÍ PŘÍKLAD

Falešný odesílatel

Jméno odesílatele lze podvrhnout.

Výhrůžka

Strach má vypnout opatrnost.

Podvodný odkaz

Neklikejte. Udělejte snímek obrazovky.

NAHLÁSIT

Nejste na to sami.
Tady je, komu zavolat.

KOMU	KDY A PROČ	KONTAKT
BANKA	Jde o peníze, přístupy do bankovnictví nebo o kartu.	**zadní strana karty, web banky**
IT TECHNIK	Pomůže počítač bezpečně vyčistit a obnovit.	**číslo mějte na papíře**
POLICIE ČR	Oznámení na kterémkoli oddělení. Akutní ohrožení: 158.	**158**
POJIŠŤOVNA	Máte kyberpojištění? Škodu hlaste bez odkladu.	**pojistná smlouva**
PODEZŘELÁ SMS	Přepošlete k prověření, číslo platí u všech operátorů.	**7726**

Kontakty si vytiskněte předem. Když je napadený počítač, telefon i e-mail, nedostanete se k nim.

SITUACE 1 · PENÍZE

Peníze v ohrožení?
Volejte banku. Hned.

Faktura vypadá normálně. Jen účet je jiný.

Už jste zaplatili?

1. Banka: zkusit zastavit platbu, blokovat přístupy.
2. Oznámení na policii, banka ho může chtít.
3. Uschovejte e-mail i fakturu.
4. Dodavateli volejte na číslo, které znáte.

Změnu účtu vždy ověřte telefonem. Nejdříve ověřujte, potom platťte.



ILUSTRAČNÍ PŘÍKLAD

SITUACE 2 · UKRADENÝ E-MAIL

Ukradený e-mailový účet otevírá skoro všechno.

Zadali jste heslo na podvodné stránce? Útočník může tiše číst poštu a čekat na příležitost.

Co udělat hned:

1. Z nenapadeného zařízení změňte heslo.
2. Odhlaste všechna zařízení a aplikace. Zapněte dvoufázové ověření.
3. Zkontrolujte přeposílání a obnovu účtu.
4. Varujte zákazníky a dodavatele před podvody.

Stejné heslo i jinde? Změňte ho všude.



ILUSTRAČNÍ PŘÍKLAD

SITUACE 3 · ZAŠIFROVANÝ POČÍTAČ

Odpojit nebo vypnout. Neplatit.

ODPOJIT	Kabel ven, Wi-Fi vypnout. Odpojte i disk se zálohou a volejte IT technika.
(NE)VYPÍNAT	Vypněte jen tehdy, když počítač nejde odpojit.
NEPLATIT	Data zpět nikdo nezaručí. S útočníky nekomunikujte.

Obnovujte s technikem z ověřené zálohy. Útočník mohl v počítači nechat zadní vrátka.



ILUSTRAČNÍ PŘÍKLAD

NÚKIB DOPORUČUJE

„Pokud je požadováno výkupné, neplaťte jej.“

SHRNUTÍ

Pět pravidel: co nedělat.



Nemazat

Smazaná zpráva je ztracená stopa.



Neplatit

Výkupné ani „bezpečný účet". Kódy z SMS nikomu.



Nečekat

Banku volejte hned. Na úplné důkazy nečekejte.



Nepoužívat napadené zařízení

Hesla přímo z něj neměňte, zálohu k němu nepřipojujte.



Nestydět se

Podvod se stane každému. Řekněte si o pomoc.

Z vašeho účtu chodily podvodné zprávy? Varujte dotčené kontakty.

POVINNOSTI SPRÁVCE OSOBNÍCH ÚDAJŮ

Incident zasáhl osobní údaje?
Posuďte riziko hned.

Patří sem i ztracený notebook s osobními údaji nebo neoprávněně změněná data. Nejste si jistí? Poraďte se s odborníkem na GDPR.

VŽDY

Zapsat

Správce zdokumentuje každé porušení zabezpečení osobních údajů a přijatá nápravná opatření.

RIZIKO PRO LIDI

Ohlásit ÚOOÚ

Bez zbytečného odkladu, pokud možno **do 72 hodin** od zjištění. Na základě posouzení rizika.

VYSOKÉ RIZIKO

Informovat lidi

Při pravděpodobném vysokém riziku správce informuje dotčené osoby bez zbytečného odkladu. GDPR zná výjimky.

Zpracováváte údaje pro klienta (třeba mzdy)? Porušení oznamte klientovi bez zbytečného odkladu.

NIS2 (v ČR zákon č. 264/2025 Sb.) se většiny živnostníků netýká. Dodáváte většímu subjektu? Čtěte smlouvu.

Redamp.io

pro podnikavé

Děkuji.
Ptejte se.

Ing. Dominik Malčík, Ph.D.
Zakladatel a CEO, Redamp.io
dominik.malcik@redamp.io • +420 724 844 313

Více o Redamp.io

redamp.io →