Občan v ohrožení - Kybernetická bezpečnost

S využitím příručky - IF CRISIS OR WAR COMES

- **Dávejte si pozor na nepravdivé informace**
- **Ochrana před škodlivým softwarem**
- **Silná hesla**
- **Bezpečné nastavení prohlížeče**
- **Jak bezpečně stahovat a používat aplikace a soubory**
- **Jak se chránit před nebezpečnými zprávami v messengerech**
- **Jak chránit data na sociálních sítích?**
- **Jak bezpečně uložit data**
- **Jak chránit děti na internetu**

Dávejte si pozor na nepravdivé informace
Státy a organizace již používají zavádějící informace, aby se pokusily ovlivnit naše hodnoty a to, jak jednáme. Cílem může být snížení naší odolnosti a ochoty se bránit.

Nejlepší ochranou před nepravdivými informacemi a nepřátelskou propagandou je **kritické zhodnocení zdroje:**

- Je to faktická informace nebo názor[1]?
- Co je cílem těchto informací?
- Kdo to vypustil?
- Je zdroj důvěryhodný?
- Jsou tyto informace dostupné někde jinde?
- Jsou tyto informace nové nebo staré a proč jsou k dispozici právě v tuto chvíli?
- Hledejte informace – nejlepší způsob, jak čelit propagandě a nepravdivým informacím, je udělat si domácí úkol.
- Nevěřte fámám – použijte více než jeden spolehlivý zdroj, abyste zjistili, zda se jedná o informace opravit.
- Nešiřte fámy – pokud informace nevypadají důvěryhodně, nepředávejte je dál.

Ochrana před škodlivým softwarem
První věc, která vám pomůže chránit vaše zařízení před viry, je instalace antivirového softwaru.
Doporučený software: Avast, ESET, McAfee, Zillya.

Jak se nenechat napadnout falešným antivirem?
Antivirový software stahujte pouze z oficiálních webových stránek vývojáře nebo z ověřených zdrojů (Play Market, App Gallery, App Store i Google Play). Pokud si nemůžete koupit placenou verzi programu, najděte si bezplatný analog, ale nestahujte cracknuté verze placených aplikací.

[1] FAKT = informace bez emocí, NÁZOR = informace plus (+) zkušenost, NÁZOR, kterému chybí informace = nevědomost, NÁZOR, který ignoruje fakta = hloupost.

Pravidelně aktualizujte svůj antivirus. Teprve poté vás program na hrozbu včas upozorní.

Antivirus je nainstalován. Co bude dál?

Pravidelně kontrolujte své zařízení, zda neobsahuje hrozby, které by mohly poškodit vaše data.

Pomocí antiviru také zkontrolujte USB klíčenky a další externí zařízení, která připojujete k počítači.

Pravidelně „resetujte“ nastavení vašeho smartphonu.

Tímto způsobem můžete neutralizovat programy „keylogger“, které sledují akce uživatele.

Neklikejte na pochybné odkazy. Jako:

- Přijaté od neznámých odesílatelů prostřednictvím e-mailu, SMS nebo messengerů a sociálních sítí;
- zprávy s výzvou k naléhavé akci a ty, které využívají vysoce relevantní a často zmiňované téma v médiích;
- ty, které vedou na pochybné stránky nebo kanály v sociálních sítích;
- ty, které nemají bezpečnostní protokol: https – bezpečné, http – potenciálně nebezpečné;
- obsahující slovo /download/ – tyto odkazy okamžitě začnou stahovat soubor. Útočníci si pravděpodobně stáhnou škodlivý kód nebo přivedou na phishingové stránky.

Dávejte pozor na ostrou a znatelnou změnu v provozu zařízení:

- **Prudké** snížení nabití, pomalý provoz, vzhled souborů, které jste nevytvořili nebo programy, které jste nenainstalovali, vzhled neznámých programů v automatickém načítání při zapnutí zařízení atd. Možná je to důsledek aktivity škodlivých programů.

Nastavte nastavení zabezpečeného messengeru.

Nastavte zabezpečené nastavení prohlížeče.

Silná hesla

Udržujte svá zařízení a účty v bezpečí. Nespolehlivá hesla – snadná kořist pro hackery a podvodníky.

Dodržujte tato jednoduchá pravidla:

- Změňte hesla na sociálních sítích, bankovních účtech a všech webových stránkách, kde mohou být vaše osobní údaje, na bezpečná. Doporučuje se měnit všechna hesla jednou měsíčně.
- Pravidelně kontrolujte, zda vaše heslo nebylo hacknuto. Zde můžete ověřit[2] - https://haveibeenpwned.com/
- Používejte správce hesel – jedná se o speciální aplikace, které uchovávají vaše hesla v zašifrované podobě a nebudete si muset pamatovat všechny složité kombinace, ale pouze heslo z aplikace samotné. (Doporučeno: 1Password, KeePassXC, Dashlane nebo manažeři v antivirových programech).
- Dvoufaktorová autentizace – je standardní dvoufázové ověření při přihlašování k účtu. Nastavit to. Poté v případě hacknutí obdržíte SMS zprávu s výzvou k potvrzení přihlášení k účtu.

[2] Jak to funguje: na webu zadejte svůj e-mail nebo telefonní číslo. Pokud byla hesla účtů registrovaných na nich hacknuta, stránka vás na to upozorní. Pokud ne, nedošlo k žádnému porušení vašich údajů.

- Chcete-li svá zařízení odemknout, nastavte přístupový kód obrazovky, vzorový klíč nebo biometrické zabezpečení (otisk prstu, ID obličeje nebo hlasové ID).
- Změňte standardní PIN kód na SIM kartu.

A jaká hesla jsou spolehlivá? Ty, které…

- **neobsahují** běžné kombinace písmen a slov; symboly, které se opakují nebo po sobě následují (0000, 1111, abc123), vaše jméno, příjmení, datum narození, jméno, příjmení nebo datum narození vašich rodičů, dětí, manžela nebo manželky,
- **místo toho** uvádějte speciální symboly, čísla, velká a malá písmena v počtu větším než 8 a také slova, která neexistují v ukrajinštině nebo angličtině a nejlépe i v jiných jazycích,
- vytvořené pomocí služby generování hesel,
- používá se pouze v jedné službě (pro každou službu nebo schránku – unikátní heslo),
- nejsou uloženy v poznámkách vašeho smartphonu nebo notebooku nebo na nálepce na notebooku stojícím uprostřed kanceláře,
- nejsou v databázi **hesel -** https://haveibeenpwned.com/Passwords
- neznají je vaši příbuzní, blízcí, kolegové,
- ta, která se výrazně liší od předchozích hesel používaných ve stejné službě.

Zabezpečené nastavení prohlížeče

Udržování prohlížečů ve funkčním stavu znamená jejich včasnou aktualizaci, stejně jako ostatní programy nainstalované v zařízení a samotný operační systém. A také – stahujte je pouze z oficiálních stránek a používejte pro ně jen minimum rozšíření.
Zde jsou indikátory, které musíte upravit ve svých prohlížečích:

- **Chrome**
  V nabídce „Nastavení“.
  Soukromí a zabezpečení – Zabezpečení – Bezpečné prohlížení – **Vylepšená ochrana**
  Soukromí a zabezpečení – Zabezpečení – Pokročilé – **Vždy používejte zabezpečené připojení**
  Stažené soubory – **Vždy určete umístění stahování**
- **Firefox**
  V nabídce „Nastavení“.
  Soubory a aplikace – **Vždy se zeptejte, kam uložit soubory**
  Soukromí prohlížeče – Zabezpečení – **Blokujte nebezpečný a podvodný obsah**
  Soukromí prohlížeče – Zabezpečení – **Povolte režim HTTPS ve všech oknech**
- **Opera**
  V nabídce „Nastavení“.
  Soukromí a zabezpečení – Zabezpečení – **Povolte ochranu před škodlivými programy a vždy používejte zabezpečená připojení**
  Stáhnout – **Před stažením se zeptejte na uložení složky**
- **Tor**
  V nabídce „Nastavení“.
  Soukromí a zabezpečení – Ochrana – Úroveň zabezpečení – **Vysoká**
  Soukromí a zabezpečení – Ochrana – Falešný obsah a Ochrana před malwarem – **Blokování nebezpečného a podvodného obsahu**
  Soukromí a bezpečnost – Ochrana – Certifikáty – **Vyžádat si potvrzení aktuálního stavu certifikátů z OCSP serverů**

Soukromí a zabezpečení – Ochrana – **Režim „Pouze HTTPS“**
Základní – Soubory a aplikace – **Vždy se zobrazí výzva k uložení souborů**

Jak bezpečně stahovat a používat aplikace a soubory
Kyberzločinci neustále vymýšlejí nové způsoby, jak oklamat uživatele škodlivými aplikacemi a programy. Stažení bezplatného filmu, hry nebo hudby – vždy existuje riziko napadení malwarem. A ziskem útočníků je získat přístup k vašim osobním údajům.
Pro zabezpečení vašich dat a zařízení dodržujte tato pravidla stahování aplikací a souborů:

- **Používejte pouze licencovaný software z ověřených zdrojů** (Play Market, App Gallery, App Store i Google Play nebo oficiální weby pro vývojáře). Věnujte pozornost tomu, kdo aplikaci publikoval, protože některé obchody mají sporné kopie oblíbených aplikací. Ruské viry se nyní často šíří prostřednictvím „pirátských“ programů.
- **Nestahujte soubory a aplikace z neznámých zdrojů** (pochybné stránky, stránky a kanály v sociálních sítích, neznámí odesílatelé).
- Potenciálně nebezpečné přípony souborů: .exe, .bin, .ini, .iso, .dll, .com, .sys, .bat, .js, .apk;
- Potenciálně bezpečné přípony souborů: .docx, .zip, .rar, .pdf.
- **Soubor byl nainstalován – zkontrolujte jej pomocí antiviru.** Nový malware nebo kód však může detekovat pouze antivirus, který je pravidelně aktualizován.
- Pokud si nemůžete koupit placenou verzi programu, **najděte si bezplatný protějšek**, ale nestahujte cracknuté verze placených programů: obvykle obsahují kód škodlivého softwaru.
- Vyberte **zákaz instalace aplikací z neověřených zdrojů a automatického stahování souborů** a pro prohlížeč – funkci „ **před každým stahováním se zeptat na umístění souboru** “. Pokud omylem kliknete na odkaz, který automaticky spustí proces stahování, nespustí se, dokud jej nepotvrdíte.
- **Vyhněte se používání aplikací od čínských a ruských vývojářů** : TikTok, VK, Odnoklassniki, Yandex.Browser, 1C, Mail.ru a další, Číňané či Rusové je mohou sledovat. Před stažením si nutně zkontrolujte informace o tom, kdo je vývojářem a vlastníkem aplikace a zda to není zakázáno.
- **Kontrolujte oprávnění,** která program vyžaduje během instalace. Ne všechny aplikace potřebují ke správnému fungování přístup k vaší geolokaci nebo osobním údajům.
- **Aktualizujte aplikace** ve smartphonu a software v počítači. Je to nutné, protože vývojáři neustále pracují na vylepšování svých bezpečnostních protokolů.

Jak se chránit před škodlivými zprávami v messengerech
Kyberzločinec se nepřestává pokoušet o kybernetické útoky. Hackeři mohou odesílat nebezpečné soubory v messengerech, které používáme.
Hackerl takové zprávy často maskuje jako zprávy pocházející údajně od státních struktur nebo bank, velkých obchodních řetězců či orgánů činných v trestním řízení.
Pamatujte: Státní struktury a agentury neposílají zprávy v messengerech s žádostí o otevření přiloženého souboru a nežádají o poskytnutí údajů o bankovních kartách, pasech, osobních účtech na sociálních sítích atd.

Zde jsou pravidla pro bezpečné nastavení oblíbených messengerů:

- **Telegram**

Otevřete nabídku „Nastavení“ a přejděte do části „Soukromí a zabezpečení“.
Vyberte v něm následující položky:
Kdo vidí telefonní číslo – **Nikdo**
Kdo najde přes číslo – **Moje kontakty**
Kdo může vidět čas mé poslední aktivity – **Nikdo**
Kdo může vidět moje profilové fotky a videa – **Moje kontakty**
Kdo se může při odesílání zpráv propojit s mým účtem – **Moje kontakty**
Kdo mi může zavolat – **Moje kontakty nebo nikdo**
V sekci „Hovory“ by měl být také Peer-to-peer nastaven na – **Moje kontakty**
(toto je možnost, která umožňuje uživatelům, kteří vám volají, přijmout nebo nepřijmout vaši IP adresu)
Kdo mě může přidat do chatů – Moje kontakty
Dvoufázové ověření – Nastavte heslo

- **WhatsApp**
  Otevřete nabídku „Nastavení“, přejděte do části „Účet“, ve které vyberte „Soukromí“.
  Vyberte následující položky:
  Naposledy online – **Nikdo**
  Profilová fotka – Moje kontakty
  Skupiny – **Moje kontakty**
  „Nastavení“ – sekce „Účet“ – **Dvoufázové ověření – Povolit**
- **Viber**
  Vyberte nabídku „Upřesnit“ a nakonfigurujte zde následující položky:
  Nastavení – Hovory a zprávy – **nastavte přepínač opačně na „Blokovat neznámé volající“**
  * „nastavit“ nebo „odstranit přepínač znamená stisknout přepínač vedle parametru. Pokud je fialová – funkce je povolena, pokud je průhledná, funkce není aktivní.
  Nastavení – Obecné – **Použít proxy server**
  Nakonfigurujte kartu „Soukromí“ následovně:
  - nastavte přepínač opačně na **" Automatická kontrola spamu** "
  - odstraňte přepínač naproti „ **peer-to-peer** “
  - nastavte přepínač opačně na „ **Požadavky** “
  - Určete, kdo vás může přidat do skupin – přejděte do „ **Nastavení pro přidání do skupin** “ a zaškrtněte políčko „ **Moje kontakty** “
  - odeberte přepínač naproti „ **Nabídněte přátelům** “
  - Osobní údaje – odstraňte přepínač naproti „ **Shromažďovat analýzy** “, „ **Povolit personalizaci obsahu** “ a „ **Povolit přesné geolokační služby** “

  Věnujte pozornost funkcím „Požádat o vaše data“ a „Smazat vaše data“ a podívejte se, jaká data o vás jsou uložena na serverech Viber.

Jak chránit data na sociálních sítích?
Soukromé informace, zejména během stanného práva, může nepřítel použít proti ukrajinským vojákům a civilistům.
Aby **byly vaše osobní účty na sociálních sítích v bezpečí, doporučujeme vám:**

- Nastavte si silné heslo pro přihlášení ke svému účtu.
- Použijte funkci dvojitého ověření. To znamená, že když se někdo pokusí přihlásit k vašemu účtu z neznámého zařízení, služba bude vyžadovat další identifikaci. V takovém případě bude na vámi zadané telefonní číslo nebo poštovní schránka odeslána zpráva s potvrzovacím kódem. Budete moci zabránit hacknutí účtu.

- Zkontrolujte nastavení svého profilu na sociálních sítích a použijte všechny možné způsoby, jak svůj účet ochránit.
- Při vytváření účtů na sociálních sítích použijte jako přihlašovací e-mailovou adresu spolehlivé služby, jako je Google nebo Yahoo.
  - Nepřihlašujte se z neznámých nebo nechráněných zařízení. Po dokončení práce se můžete zapomenout odhlásit ze svého účtu nebo si zařízení může pamatovat přihlašovací jméno a heslo, které jste použili při přihlášení. Kromě toho může být zařízení infikováno malwarem, který shromažďuje a přenáší hesla a přihlašovací údaje třetím stranám.
  - Neotevírejte přílohy zpráv od podezřelých nebo neznámých lidí. Ostatně phishing je pro zločince nejběžnějším způsobem, jak získat hesla k poštovním schránkám a účtům na sociálních sítích.
  - Nainstalujte si do zařízení antivirové programy. Pomohou vám chránit se před viry.

Jak bezpečně ukládat data

- Uchovávejte důležité osobní soubory zašifrované nebo ve skrytých složkách a albech. Pro tohle:
  - **Pro zařízení Samsung** : použijte tajnou složku **Knox .** Můžete do něj přenést některé aplikace, fotografie a další obsah.
    Pro všechna zařízení Android : Galerie – Alba – stiskněte a podržte požadované album – v doplňkovém menu vyberte **Skrýt** Nebo: Galerie – Alba – posuňte prst po obrazovce shora dolů – otevře se skrytá složka, do které je potřeba nastavit heslo nebo grafický klíč.
    Nebo funkce „Druhé úložiště“ (k dispozici na některých zařízeních Android)
  - **Pro iPhone, iPad nebo iPod touch:** Fotografie – vyberte fotografii nebo video, které chcete skrýt, – stiskněte tlačítko více – Skrýt – potvrďte.
- **K výměně informací a korespondence používejte šifrování.** Pro E-mail to může být asymetrické PGP šifrování, na které existují speciální programy, a pro messengery – šifrované chaty a zprávy, které po chvíli zmizí. Vaše data tak zůstanou soukromá, pokud bude váš počítač, telefon nebo e-mailový účet napaden. Hackeři nebudou moci číst vaše zprávy bez šifrovacího klíče.
- **Uchovávejte kopie důležitých souborů v cloudovém úložišti.** Například Dropbox, OneDrive, Google Drive atd. Odtud budete moci obnovit data, pokud bude telefon jailbreaknut. Důležité dokumenty také zálohujte na samostatná zařízení nebo zabezpečené cloudové úložiště. Když hackeři získají přístup k zařízení, není vždy možné informace obnovit.
- **Neukládejte do paměti smartphonu informace, které by vám mohly ublížit** v případě zaměstnání a hledání. Okamžitě smažte takové soubory a chaty z paměti smartphonu. A co je důležité zachovat, předběžně stáhnout do cloudového úložiště.
-

Jak chránit dítě na internetu

Je důležité dětem vysvětlit, že internetová bezpečnost je stejně důležitá jako pravidla bezpečného chování v reálném životě.

Hlavním pravidlem je mluvit se svými dětmi o kybernetické bezpečnosti:

- Nezapomeňte, že nemůžete zveřejňovat soukromé fotografie, zveřejňovat osobní údaje (adresu, telefonní čísla a další osobní údaje) na sociálních sítích, v komunikaci v messengerech a chatech a také se účastnit online průzkumů.

- Připomeňte si riziko zachycení virů při otevírání podezřelých odkazů, příloh, souborů. Pomozte svému dítěti nainstalovat potřebné programy pro ochranu a nakonfigurovat všechny jeho gadgety.
- Dohodněte si časové limity pro hry na smartphonu a surfování po internetu a sledujte jejich dodržování
- Diskutujte o informacích, které vaše dítě čte na internetu. Mluvte o padělcích.
- Naučte své dítě vytvářet spolehlivá hesla a s nikým je nesdílet.

Můžete také pravidelně kontrolovat, jaké stránky vaše dítě navštěvuje: to lze provést pomocí karty „Historie“ v prohlížeči. Dbejte však na to, aby se dítě nebálo, když na počítači nebo chytrém telefonu udělá „něco špatně“. V případě jakýchkoli nestandardních situací byste je neměli skrývat, ale okamžitě vyhledat pomoc.
A pamatujte: přísná prohibice obvykle nefunguje. Mnohem důležitější je vybudovat si vztah založený na důvěře a naučit dítě zodpovědnosti a opatrnosti na internetu.