Pravidla hry Black Hat Hacker

Počet hráčů: min. 2 hráči
Počet karet: 23 (11 dvojic + 1 karta Black Hat Hackera)

Příprava hry: Karty se zamíchají a rozdají mezi hráče. Každý si prohlédne své karty v ruce a ihned vyloží všechny páry na stůl.

Průběh hry: Začíná hráč nalevo od rozdávajícího. Ten si naslepo vytáhne jednu kartu od hráče napravo, pokud s ní vytvoří pár, ihned ho vyloží. Hra pokračuje po směru hodinových ručiček, dokud se hráči postupně nezbaví všech karet.

Cíl hry: Cílem je se co nejdříve se zbavit všech karet. Prohrává ten, kdo jako poslední drží v ruce nepárového Černého Petra - Black Hat Hackera.

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

BLACK HAT HACKER

ZLÝ HACKER, KTERÝ VYUŽÍVÁ SVÉ ZNALOSTI KE ŠPATNÝM ÚČELŮM. NAPADÁ SYSTÉMY, KRADE DATA A ZPŮSOBUJE ŠKODY.

NADMĚRNÉ SDÍLENÍ

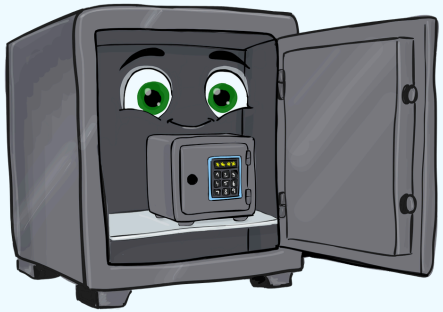
ČASTÉ A NEUVÁŽENÉ SDÍLENÍ OSOBNÍCH INFORMACÍ, FOTEK A OBSAHU MŮŽE VÉST KE ZTRÁTĚ SOUKROMÍ, ZNEUŽITÍ DAT A VZNIKU TRVALÉ DIGITÁLNÍ STOPY.

OCHRANA SOUKROMÍ

SOUKROMÉ PROFILY NA SÍTÍCH A OMEZENÍ OPRÁVNĚNÍ APLIKACÍ SNIŽUJÍ RIZIKO ZNEUŽITÍ. DŮLEŽITÉ JE I MYSLET NA TO, CO VŠECHNO SDÍLÍME.

KRÁDEŽ HESLA

HESLO MŮŽE BÝT ZÍSKÁNO PODVODEM NEBO PŘI ÚNIKU DAT. JEHO ZNEUŽITÍ PAK MŮŽE VÉST K NEOPRÁVNĚNÉMU PŘÍSTUPU K ÚČTU.



VÍCEFAKTOROVÉ OVĚŘENÍ

K PŘIHLÁŠENÍ JE KROMĚ HESLA POTŘEBA JEŠTĚ DALŠÍ OVĚŘENÍ, NAPŘÍKLAD JEDNORÁZOVÝ KÓD. ÚČET JE TAK CHRÁNĚN VÍCE ZPŮSOBY.

INFIKOVANÁ APLIKACE

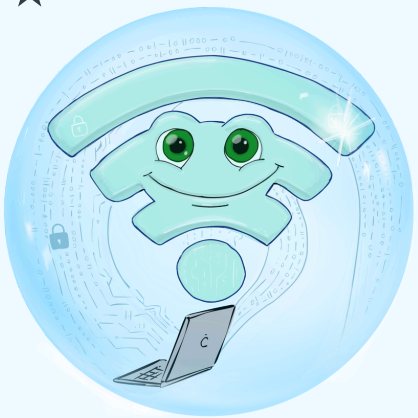
PROGRAMY Z NEDŮVĚRYHODNÝCH WEBŮ MOHOU OBSAHOVAT VIRUS. TEN MŮŽE POŠKODIT ZAŘÍZENÍ NEBO KRÁST DATA.

DŮVĚRYHODNÝ OBCHOD

APLIKACE JE VHODNÉ INSTALOVAT JEN Z DŮVĚRYHODNÝCH ZDROJŮ, NAPŘÍKLAD Z GOOGLE PLAY, APP STORE NEBO MICROSOFT STORE.

VEŘEJNÁ WI-FI SÍŤ

VEŘEJNÉ WI-FI SÍTĚ V KAVÁRNÁCH NEBO NA NÁDRAŽÍ NEJSOU VŽDY BEZPEČNÉ A NĚKDO NA STEJNÉ SÍTI MŮŽE SLEDOVAT PŘENÁŠENÁ DATA.

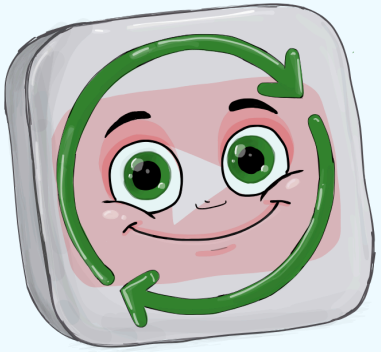


VPN

VPN VYTVÁŘÍ ŠIFROVANÉ PŘIPOJENÍ K INTERNETU, TAKŽE OSTATNÍ NA STEJNÉ WI-FI NEVIDÍ PŘENÁŠENOU KOMUNIKACI.

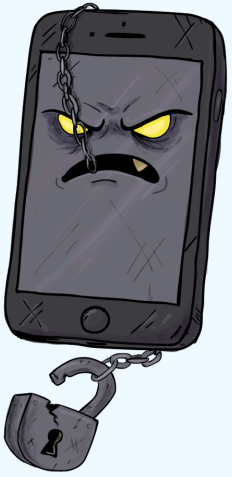
ZASTARALÁ APLIKACE

STARŠÍ VERZE APLIKACÍ MOHOU OBSAHOVAT BEZPEČNOSTNÍ CHYBY, KTERÉ ÚTOČNÍCI ZNEUŽÍVAJÍ K NAPADENÍ ZAŘÍZENÍ.



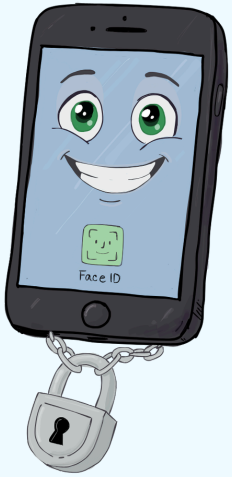
PRAVIDELNÉ AKTUALIZACE

AKTUALIZACE OPRAVUJÍ CHYBY A ZLEPŠUJÍ ZABEZPEČENÍ. PRAVIDELNÝM AKTUALIZOVÁNÍM SE SNIŽUJE RIZIKO NAPADENÍ.



ODEMČENÝ TELEFON

POKUD TELEFON NEMÁ ZÁMEK, MŮŽE HO KDOKOLIV SNADNO OTEVŘÍT A PROHLÍŽET ZPRÁVY, FOTKY NEBO SPOUŠTĚT APLIKACE.



UZAMČENÝ TELEFON

TELEFON JE VHODNÉ CHRÁNIT ZÁMKEM, AŤ UŽ PINEM, HESLEM, GESTEM, OTISKEM PRSTU NEBO FACE ID. TELEFON PAK ODEMKNE POUZE JEHO MAJITEL.

SLABÉ HESLO

KRÁTKÁ NEBO JEDNODUCHÁ HESLA JAKO „123456" NEBO „HESLO" LZE SNADNO UHODNOUT. ÚTOČNÍK SE TAK MŮŽE RYCHLE DOSTAT DO ÚČTŮ.

SILNÉ HESLO

BEZPEČNÉ HESLO BY MĚLO MÍT ALESPOŇ 12 ZNAKŮ. IDEÁLNÍ JE KOMBINACE VELKÝCH A MALÝCH PÍSMEN, ČÍSLIC A SPECIÁLNÍCH ZNAKŮ.

RANSOMWARE

ŠKODLIVÝ PROGRAM, KTERÝ ZABLOKUJE PŘÍSTUP K DATŮM V POČÍTAČI. ÚTOČNÍK PAK POŽADUJE ZAPLACENÍ ZA JEJICH ODEMKNUTÍ.

ZÁLOHOVÁNÍ DAT

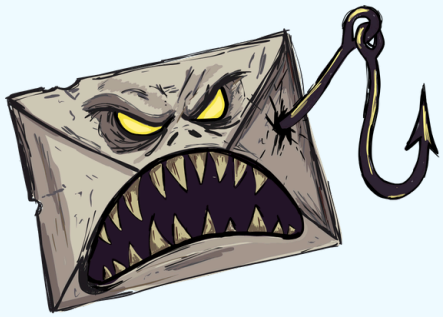
DŮLEŽITÁ DATA JE VHODNÉ UKLÁDAT I NA JINÉ MÍSTO. PŘI ZAŠIFROVÁNÍ RANSOMWAREM JE LZE OBNOVIT ZE ZÁLOHY BEZ PLACENÍ VÝKUPNÉHO.

MALWARE

ŠKODLIVÝ PROGRAM, KTERÝ SE DOSTANE DO ZAŘÍZENÍ BEZ VĚDOMÍ UŽIVATELE. MŮŽE KRÁST DATA, SLEDOVAT AKTIVITU NEBO POŠKODIT ZAŘÍZENÍ.

ANTIVIRUS A FIREWALL

ANTIVIRUS HLÍDÁ ZAŘÍZENÍ ZEVNITŘ A HLEDÁ ŠKODLIVÉ PROGRAMY. FIREWALL HLÍDÁ ZVENKU A BLOKUJE PODEZŘELÁ PŘIPOJENÍ DO ZAŘÍZENÍ.



PHISHINGOVÝ E-MAIL

PODVODNÁ ZPRÁVA, KTERÁ SE VYDÁVÁ ZA DŮVĚRYHODNÝ ZDROJ A SNAŽÍ SE PŘIMĚT UŽIVATELE KLIKNOUT NA ODKAZ NEBO ZADAT CITLIVÉ ÚDAJE.

KONTROLA ODESÍLATELE

PŘED OTEVŘENÍM ODKAZU JE VHODNÉ ZKONTROLOVAT ADRESU ODESÍLATELE. POKUD SE ZDÁ PODEZŘELÁ, ZPRÁVU RADĚJI IGNORUJTE.

STEJNÉ HESLO VŠUDE

POUŽÍVÁNÍ JEDNOHO HESLA PRO VÍCE SLUŽEB JE RIZIKOVÉ. POKUD UNIKNE, ÚTOČNÍK ZÍSKÁ PŘÍSTUP K VÍCE ÚČTŮM.

UNIKÁTNÍ HESLA

KAŽDÝ DŮLEŽITÝ ÚČET BY MĚL MÍT VLASTNÍ UNIKÁTNÍ HESLO. POKUD JEDNO HESLO UNIKNE, ÚTOČNÍK SE NEDOSTANE DO OSTATNÍCH ÚČTŮ.