eset | bezpečne na nete

11 krokov ako ochrániť chytré zariadenia

1. Používajte kvalitný bezpečnostný softvér na ochranu pred internetovými hrozbami.
2. Uistite sa, že je operačný systém a bezpečnostný softvér vo vašich zariadeniach aktualizovaný.
3. Zabezpečte váš router silným heslom a nezabúdajte na pravidelnú aktualizáciu.
4. Zabezpečte vaše zariadenia dostatočne silnými heslami – PIN, touch ID, uzamknutie kódom alebo vzorom a podobne.
5. Aktivujte si možnosť dvojfaktorového overovania pri prihlasovaní do online služieb.
6. Majte zapnutú bránu firewall, ktorá blokuje akýkoľvek prístup k počítaču.
7. Vykonávajte pravidelnú zálohu vašich zariadení.
8. Zabezpečte vašu domácu sieť dostatočne silným heslo. Naprihlasovanie do online bankingu alebo na nákupy používajte zabezpečenú sieť alebo dátové pripojenie.
9. Na prihlasovanie do sociálnych sieti, e-shopov, online bankingu ainých aplikácií používajte v prípade mobilných zariadení oficiálne aplikácie.
10. Správajte sa zodpovedne. Neklikajte na podozrivé odkazy a neotvárajte prílohy v nevyžiadanej pošte.
11. Aplikácie sťahujte len z oficiálnych obchodov. Pred inštaláciou si skontrolujte povolenia, ktoré aplikácia požaduje.

eset | bezpečne na nete

Ako zabezpečiť router?

Krok 1
Zmena hesla

Zmeňte predvolené heslo od dodávateľa po jeho zakúpení. Nové heslo či fráza by mala byť dlhá a zložitá, a odlišná od prihlasovacích údajov do iných zariadení a služieb. Pokiaľ máte problém so zmenou, kontaktujte dodávateľa.

Krok 2
Pravidelný audit všetkých chytrých zariadení

Viete koľko zariadení je pripojených do vašej domácej siete? Pokiaľ nie, môžete uskutočniť vlastný audit. Postup, ako na to, nájdete na www.bezpecnenanete.sk.

Krok 3
Testy zraniteľností

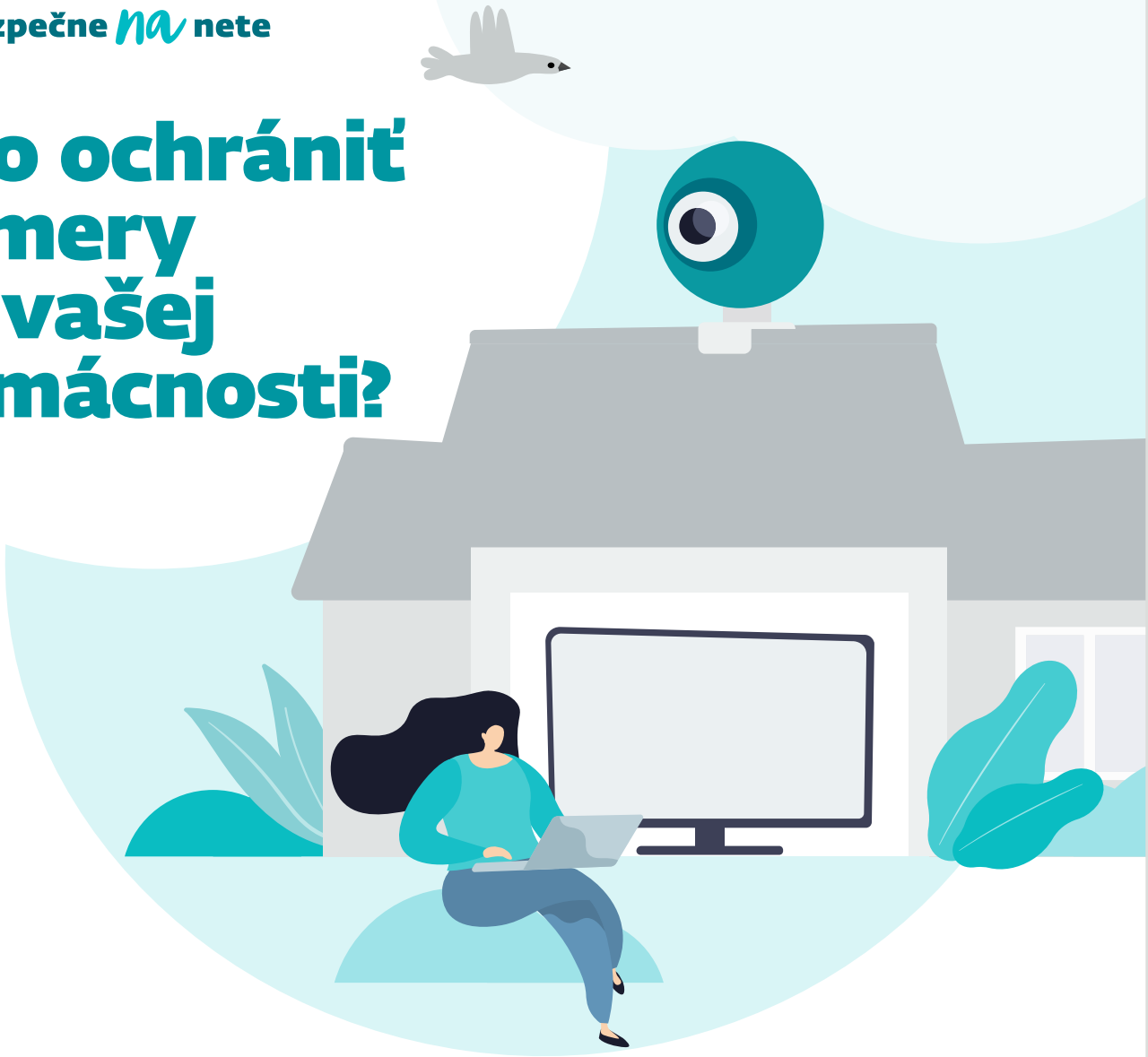
Pre zistenie slabých miest v nastaveniach môžete vykonať testy zraniteľností. Tie sa vykonávajú pomocou nástrojov, ktoré prostredníctvom automatizovaných úloh hľadajú známe zraniteľnosti.

Krok 4
Aktualizácie

Router je vo svojej podstate ako počítač. Takže jeho operačný systém, zabudovaný ako firmvér, musí byť pravidelne aktualizovaný z dôvodu prípadných bezpečnostných zraniteľností. Odporúčame vám pravidelne kontrolovať dostupnosť nových aktualizácii, aspoň niekoľkokrát za rok.

bezpečne na nete

Ako ochrániť kamery vo vašej domácnosti?



Žiaden systém nie je stopercentný

V prípade kamier vdomácnosti sa oplatí radšej investovať do kvality.

Ak je to možné, kameru odpojte

Ak kameru nepoužívate, odpojte ju. Ak je to možné, vypnite vzdialené sledovanie pomocou pripojenia k internetu.

Neposkytujte informácie, ktoré nemusíte

Bezpečnostné kamery umiestnite tak, aby záber neposkytoval ďalšie podrobnosti o vašej totožnosti alebo vašej polohe.

Zabezpečte všetky vaše zariadenia – počítač, smartfón či smart televízor

Používajte kvalitný bezpečnostný softvér, ktorý vás ochráni pred najnovšími druhmi malvéru a poskytuje funkciu ochrany webovej kamery.

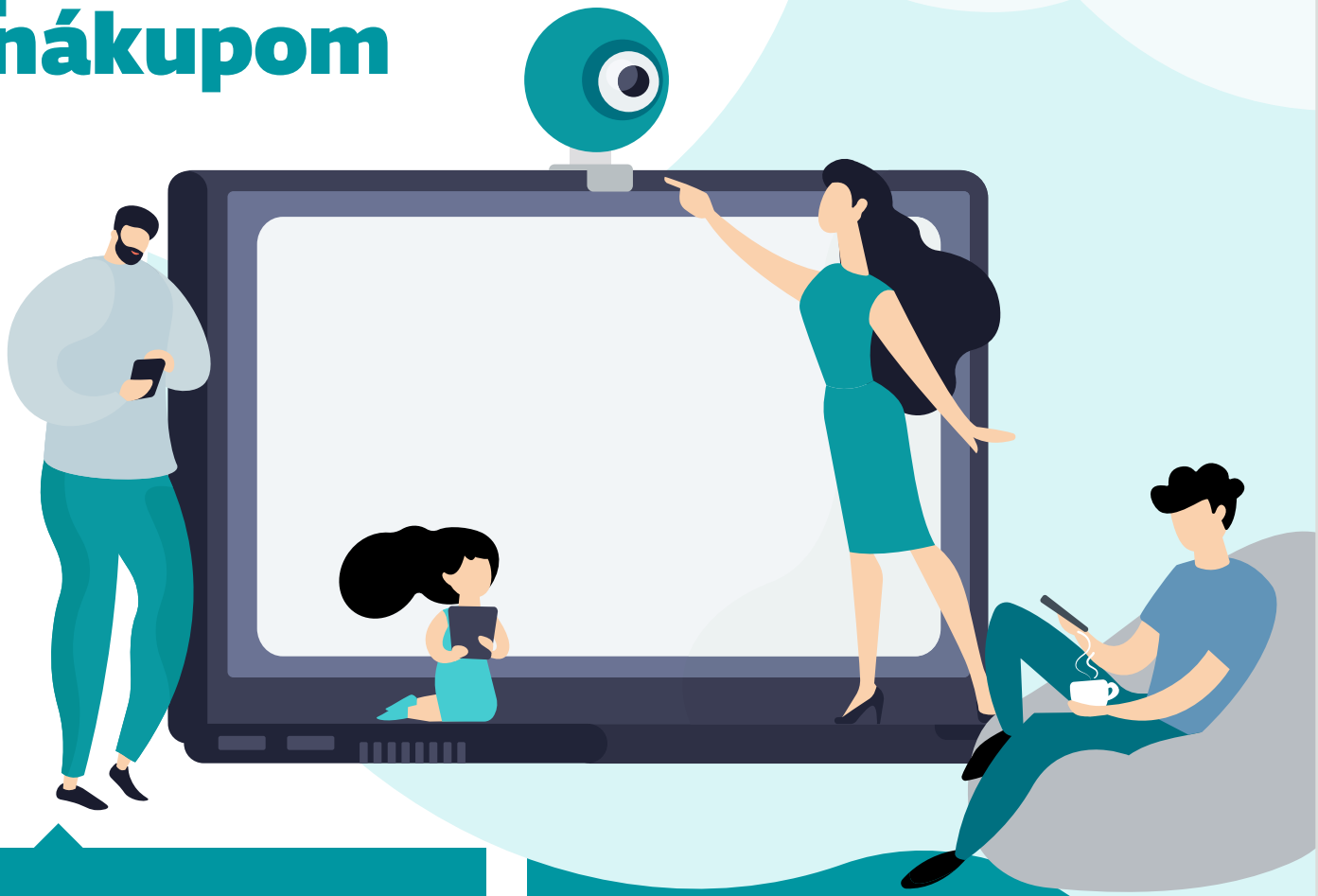
Nezabúdajte na registráciu

„Otvorenými dverami“, ktoré umožňujú kybernetickým útočníkom ovládať vaše kamery, je v tomto prípade firmvér, ktorý nebol správne aktualizovaný. Najjednoduchší spôsob jeho zabezpečenia je registrácia kamery u výrobcu.

Zmena hesla

Kamera by sa nemala používať bez toho, aby ste na nej najskôr zmenili heslo. Nové zložité heslo alebo frázové heslo je najlepšiou voľbou. Ideálne je používať kombináciu veľkých a malých písmen, číslic a znakov.

Odporúčania pred nákupom



Odporúčanie 1

Pred nákupom kamery do vašej domácnosti si preverte, aké značky a typy sú momentálne na trhu dostupné a akými vlastnosťami disponujú. Nenakupujte len na základe ceny.

Odporúčanie 2

Pred nákupom vám odporúčame vyhľadať si prípadné bezpečnostné chyby nájdené v zariadeniach výrobcu, od ktorého chcete kameru zakúpiť. Ak na ňu v minulosti vydal záplatu a aktualizáciu, je vysoká šanca, že to spraví opäť. Ak sa tváril, že sa nič nedeje a chybu neuznal, odporúčame vám nájsť si produkt od iného výrobcu.

Odporúčanie 3

Pred nákupom si prečítajte podmienky používania zariadenia. Mali by ste sa z nich dozvedieť napríklad to, aké osobné údaje zariadenie zbiera, či je záznam prenášaný online aj šifrovaný a či je vôbec možné zariadenie aktualizovať.

Nešifrovaný prenos kamerového záznamu a absencia možnosti aktualizovať firmvér zariadenia by vás mali od kúpy odradiť.

eset | bezpečne na nete

Smart TV ako terč kybernetických útočníkov?

Tipy, ako ju zabezpečiť.

Starajte sa o svoj router

Router je vstupnou bránou do vašej siete. Router, o ktorý sa dobre nestaráte, predstavuje bezpečnostné riziko nielen pre vašu domácu sieť, ale aj smart televízor. Ako sa správne starať o váš router? Všetky tipy nájdete na www.bezpecnenanete.sk.

Aktualizujte

Smart televízor, podobne ako aj iné chytré zariadenia, majú firmvér. Ten sa musí pravidelne aktualizovať, aby ste predišli chybám a zraniteľnostiam.

Používajte kompletné bezpečnostné riešenie

Rovnako, ako váš počítač alebo mobilný telefón, musí byť aj smart televízor chránený. Na ochranu týchto zariadení by ste preto mali používať kompletné bezpečnostné riešenie od dôveryhodného poskytovateľa.

Sťahujte aplikácie priamo z obchodu Google Play alebo App Store

Pred stiahnutím aplikácie vždy skontrolujte meno vývojára, počet inštalácií a hodnotenia ostatných používateľov.

Konfigurácia

Smart televízor musí byť správne nakonfigurovaný, aby sa zaistila jeho bezpečnosť a funkčnosť.

1. Skontrolujte nastavenia ochrany osobných údajov a informácií, ktoré povoľujete dodávateľovi zbierať, prípadne zdieľať s tretími stranami.
2. Ak váš smart televízor obsahuje aj kameru a tú nepoužívate, jednoducho ju vypnite.