КАКО ДА ГИ ЗАШТИТИТЕ ВАШИТЕ ЛИЧНИ ПОДАТОЦИ ОД КРАЖБА И ЗЛОУПОТРЕБА?

1. Периодично креирајте сигурносна копија на податоците на надворешна меморија или облак.

2. Задолжително користете антивирусни програми и редовно ажурирајте ги и надградувајте ги антивирусните и други безбедносни алатки.

3. Надградете ги и ажурирајте ги оперативните системи и сите апликации на вашиот компјутер со најновите верзии.

4. Не отворајте е-пошти што пристигнуваат од сомнителни адреси, невообичаени домени, особено не отворајте сомнителни прилози на е-пошти кои имаат невообичаена форма, содржат невообичаени изрази, имаат многу граматички грешки или текстот делува како лош превод или не во духот на македонскиот јазик **(**на пр. „прикачен е на вашето читање**“)**.

5. Проверете го испраќачот на е-поштата пред да **ја** отворите. Ако идентитетот на вашиот испраќач е сомнителен, не отворајте **ја** е-поштата**!** (пр. **amagnus@india.com)**.

6. Обрнете внимание на екстензијата на датотеката во прилогот, не отворајте прилози со необични екстензии како што се **as.jar,.ace**.

7 Ако е-поштата што ја добивте содржи сомнителна **URL**-адреса, поминете со глувчето преку **URL**-адресата во поштата, но не кликнувајте! Треба да ја видите вистинската **URL** адреса на која ќе бидете пренасочени. Ако изгледа сомнително или завршува како **.exe, .js** или **.zip**, не отворајте го линкот!

8 Кога ќе завршите со користењето на вашиот профил на социјалната мрежа, е-пошта или друга услуга на интернет, одјавете се. Ако останете најавени и продолжите да сурфате, тоа е исто како да ја оставите отклучена вашата куќа: им ја олеснувате работата на хакерите и уценувачите. Затоа, избегнувајте ги ризиците и одјавете се од вашите сметки пред да продолжите да ја прелистувате веб страницата!

9 Внимавајте на понуди кои се „премногу добри за да бидат вистинити“ на непроверени и непознати е-продавници. Купувајте само во проверени е-продавници, читајте рецензии, ако плаќате со кредитна картичка плаќајте само преку проверени даватели на услуги за плаќање, бидете многу внимателни ако некој ве замоли да му ги испратите вашите лични податоци или ви испрати линк до сомнителни веб страници! Ова може да биде „фишинг“ напад со цел да се украдат вашите лични податоци и вашите пари!

10 Кога плаќате на интернет, не користете отворена или бесплатна **Wi-Fi** (Вај-фај) мрежа, туку користете само безбедна **Wi-Fi** мрежа.

SCAN ME

Овој проект е финансиран од Европската Унија