ТОП 10 НАЧИНИ КАКО ДА БИДЕТЕ БЕЗБЕДНИ ONLINE КАКО ПОТРОШУВАЧ

ОПМ
Организација на потрошувачите на Македонија

Министерство за Економија

Интернетот ни нуди огромен спектар на можности и избор. Лесно можеме да се поврземе и да комуницираме со семејството и пријателите од целиот свет, да го извршиме нашето неделно пазарување и да го спроведеме плаќањето на нашите сметки со еден клик, заштедувајќи време и пари. Сите овие активности на некој начин ги користат нашите лични информации – нашите информации во банка за да извршиме уплата, нашите слики и коментари, нашите адреси за доставување. Со повеќе податоци за нас онлајн, ризиците од крадење на идентитетот, хакирање, уцена и измама се зголемуваат.

Еве неколку едноставни работи кои сите ние можеме да ги направиме за да ги заштитиме нашите лични податоци онлајн и да уживаме во интернетот чувствувајќи се сигурно:

1. Користете различни и оригинални лозинки

- Ова е нешто кое најлесно може да се промени, но и нешто кое никој од нас не го прави. Од огромна важност е да се има различен пин или лозинка за секое корисничко име за дури и кога ќе дојдеме во ситуација едно корисничко име да ни е хакирано, останатите да можат да ни останат заштитени. Најважната лозинка која треба редовно да ја менуваме е онаа на е-поштата бидејќи таа може да ја користиме за да ги промениме лозинките на останатите кориснички имиња. Ако се сомневате дека сте жртва на хакирање (а често не сме свесни за тоа), сменете ја лозинката веднаш и сменете ги сите останати исти лозинки кои ги имате.
- Избегнувајте користење на очигледни лозинки, како вашето место на раѓање или името на вашето дете, бидејќи овие податоци лесно се дознаваат. Наместо тоа. користете комплицирани зборови или фрази кои содржат големи букви, бројки и интерпункциски знаци за дополнителна сигурност. Размислете за користење на сервис за лозинки кој ќе ги заштити сите ваши лозинки со тоа што ќе треба да запомните само една.

2. Искористете ги алатките за безбедност

- Повеќето од компаниите им нудат огромен спектар на опции на потрошувачите во однос на безбедносните алатки, како алатки за безбедност и лозинки. Секогаш треба да имате лозинка на вашиот смартфон – зачудувачки е бројот на луѓе кои немаат – без него сите ваши апликации, карти, календари, контакти, информации околу плаќањата и огромен број на лични податоци стануваат достапни за читање. Одвојте време за да ги прочитате алатките за приватност и подесете ги според вашата склоност и не се срамете да побарате помош ако наидете на проблем правејќи го тоа.

3. Бидете претпазливи што споделувате на социјалните мрежи

- Ако се придржувате до зададените подесување, тогаш до сè што споделувате може да има увид кој било и каде било, затоа размислете пред да спо-

делите. Одвојте време да ги прочитате алатките за приватност и избегнете споделување на лични информации кои би направиле целосна слика за вас, како вашата адреса, работно место, планови за одмор и имиња на блиски членови од семејството.

4. Внимавајте на ви-фи

- Бесплатното јавно ви-фи е многу погодно, но безбедноста може да биде проблем кога споделувате мрежа со голем број на луѓе. Користете „https“ доколку сте на ви-фи мрежа кога се вклучувате на вашата е-пошта, социјални мрежи и останати лични кориснички адреси. Доколку сте во вашиот дом, секогаш имајте лозинка за влез во вашата мрежа.

5. Не дозволувајте да бидете измамени од лажни е-пошти или СМС и останати пораки

- Лесно е да бидете поведени од писмо на е-пошта кое тврди дека ви следуваат пари како награда или одамна изгубен дел од наследство, но внимавајте! Не верувајте на понуди или награди кои звучат премногу добро за да бидат вистинити бидејќи најверојатно и се. Ако добиете писмо на е-пошта кое вели дека ви следува огромна сума на пари и мора да обезбедите детали од вашата банкарска сметка за да ги добиете – внимавајте! Ова е лесен начин за хакери да ги добијат вашите банкарски информации и да извршат измама.

- Ако добиете писмо на е-пошта од вашата банка или компанија во која се бараат вашите информации, проследете го писмото до нивната служба за е-пошта за да се осигурите дека ова тврдење е вистинито пред да дадете какви било информации.

6. Избегнувајте отворање на прилози кон е-пошта или необични линкови

- Вирусите најчесто се праќаат преку прилози во е-пошта или линкови. Вирусите можат да му наштетат на вашиот уред и да си обезбедат влез до вашите лични податоци. Доколку не го препознавате испраќачот или не знаете што е прилогот кон е-поштата, не го отворајте. Истото важи дури и за линкови од вашите пријатели. Ако ви било испратено нешто што ви изгледа малку чудно, а е корисничко име на ваш пријател, секогаш прашајте ги за тоа пред да го отворите бидејќи е многу возможно нивната е-пошта да била хакирана.

7. Користете привремена е-пошта

- Кога се приклучувате на некоја веб-страница често од вас се бара да дадете податоци за вашата е-пошта и контакт-информации, дури и ако само еднаш ги користите услугите. Доколку сакате да избегнете добивање на е-писма за маркетинг и продажба, можете да користите привремена е-пошта. Ова ви пружа доволно време да се при-

клучите и да ги добиете бараните податоци. Е-поштата потоа автоматски се уништува без да ги зачува вашите лични податоци. Користењето на привремени е-пошти нуди безбеден начин на приклучување кон веб-страници без да ја откриете вашата вистинска е-пошта. Има многу веб-страници кои ја нудат оваа услуга, само пребарајте го терминот „temporary email addresses“ за да ги откриете нивните можности.

8. Осигурете се дека вашите плаќања се безбедни

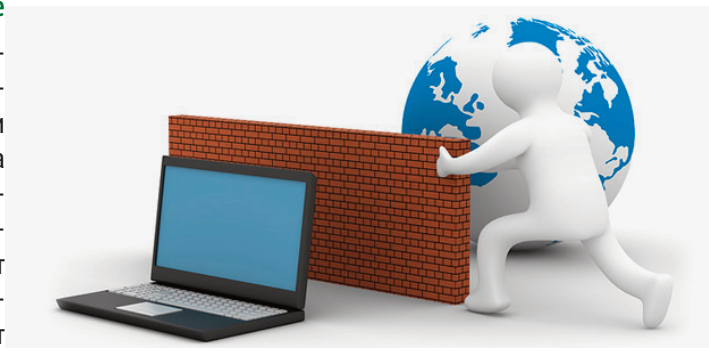
- Кога вршите плаќање онлајн, барајте веб-адреси кои започнуваат со „https://“, не само „http“, буквата „S“ (на латиница) означува сигурност. Ова значи дека податоците се дешифрирани додека патуваат помеѓу веб-страницата и вашиот компјутер. Исто така, треба да има икона во форма на зелен катанец на левата или десната страна покрај името на веб-адресата што укажува на тоа дека веб-страницата е безбедна.

- Полезно е да си создадете навика редовно да ги проверувате вашите сметки и извештаи од банка по извршување на секоја уплата за да се осигурите дека вистинската сума била депонирана и дека при вршењето на трансакцијата немало никаква измама.

9. Редовно вршете обновување на софтверот

- Вклучувањето на автоматски обновувања на вашиот оперативен систем и софтвер е навистина лесен начин да се осигурите дека ја имате најдобрата достапна заштита така што секое обновување нуди дополнителна безбедност автоматски. Доколку имате стар софтвер, нему ќе му недостасуваат најновите заштити, па затоа вклучете ги автоматските обновувања на сите ваши уреди.

10. Инсталирајте ги и обновете ги заштитните ѕидови (firewalls), антивирусот и софтверот против шпионирање



- Важно е да се има ова подесување на сите ваши уреди бидејќи заштитните ѕидови спречуваат неовластени лица да го хакираат вашиот компјутер, софтверот против шпионирање го штити вашиот компјутер од вируси и шпионирачки програми да имаат увид во вашите лозинки, кориснички адреси и лични податоци. Без ова вашите уреди се подложни на огромен ризик да бидат хакирани.