Ostanite opušteni i nakon odmora

1. Razmislite dvaput na društvenim mrežama
Društvene mreže sjajne su za ostajanje u vezi s ljudima koje volimo. Ipak, uvijek biste trebali razmišljati o onome što objavite na mreži. Poštujte privatnost drugih ljudi i preuzmite kontrolu nad dostupnim informacijama koje pružate.

2. Pazite na online igre
Besplatne online igre često skrivaju zlonamjerni softver. Često su vaši osobni podaci "naknada" koju plaćate za igranje, pa nemojte davati svoje osobne podatke za nekoliko minuta zabave.

3. Izbjegavajte otvoreni WiFi
Otvorene WiFi mreže mogu biti zamke koje hakeri koriste za krađu vaših podataka, izbjegavajte ih kad je to moguće!

4. Budite pametni u pogledu lozinki
Lozinke su glavna obrana vaših računa. Trebali biste koristiti različite lozinke za svaki račun i često ih mijenjati; možete koristiti pouzdanog upravitelja zaporki da biste to olakšali. Kad god je to moguće, koristite provjeru autentičnosti u dva koraka.

5. Provjerite postavke privatnosti
Uvijek provjerite postavke privatnosti svojih aplikacija: ako se od vas traže nepotrebna dopuštenja (na primjer, aplikacija za vremensku prognozu koja zahtijeva čitanje kontakata ili pristup kameri), samo recite ne!

6. Prepoznajte svoju neželjenu poštu i lažnu e-poštu
Pažljivo provjerite svu e-poštu koju primite: možda ste meta spama ili krađe identiteta. Obratite pažnju na e-poštu pošiljatelja i nikad ne otvarajte privitke ako niste 100% sigurni da je to sigurno.

7. Koristite antivirusne i zaštitne programe
Antivirusni softver i vatrozidi mogu spriječiti da vaši uređaji budu zaraženi zlonamjernim softverom ili da ih napadnu hakeri, stoga ih ažurirajte! Ali zapamtite također da antivirusni softver nije savršen - uvijek razmislite prije klika!

8. Izradite sigurnosnu kopiju podataka
Koliko su vam važni vaši podaci? Zamislite da vam je ukradeno računalo ili je pametni telefon izgubljen; biste li požalili što nemate sigurnosnu kopiju?

9. Budite spremni na hakiranje
Je li vaš račun ugrožen? Ne čekajte, odmah poduzmite akciju! Promijenite svoje lozinke što je prije moguće i obavijestite svoju banku ako postoje podaci o plaćanju.

10. Odjavite se
Uvijek se odjavite s računa nakon što koristite javno računalo.

11. http ili https?
Jeste li se ikad zapitali koja je razlika između http i https u adresama web mjesta? 's' znači sigurno, što znači da je kriptirano. Ako ne vidite 's', ne dajte nikakve osobne podatke - posebno ne za plaćanja.

Bello CONSULTING
DPO: William Bello
email: dpo@bello.hr