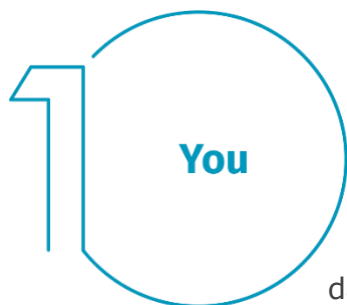


Cele mai importante 5 măsuri de Securitate pentru lucrul de acasă

Ne dăm seama că lucrul de acasă poate fi o noutate pentru unii, iar adaptarea la noul mediu poate fi copleșitoare. Unul dintre obiectivele noastre este să vă oferim posibilitatea de a lucra în siguranță de acasă. În continuare prezentăm cinci pași simpli pentru a putea lucra în siguranță. Partea cea mai bună a acestora este că vă ajută nu doar să lucrați în siguranță, ci și să vă apărați căminul împotriva infractorilor cibernetici.



Dvs.: cel mai important lucru de știut este că, singură, tehnologia nu vă poate apăra. Dvs. sunteți cea mai bună apărare. Atacatorii și-au dat seama că îți ating scopul mai ușor dacă vă abordează pe dvs. în loc să vă atace computerul sau celelalte dispozitive. Dacă vor o parolă, datele cu care lucrați sau controlul asupra computerului dvs., vor încerca să le obțină păcălindu-vă. De multe ori fac acest lucru inducând un sentiment al urgenței extreme. De exemplu, vă sună, se prezintă drept angajați ai biroului de asistență tehnică Microsoft și susțin că vi s-a infectat computerul. Sau vă trimit un avertisment prin e-mail că un pachet nu a putut fi livrat, ca să vă convingă să faceți clic pe un link nociv. Cele mai frecvente semne ale atacurilor de inginerie socială sunt:

- Cineva prezintă o situație extrem de urgentă, de multe ori provoacă frică, intimidează, invocă o criză sau un termen limită important. Atacatorii cibernetici se pricep să creeze mesaje convingătoare, care par să vină de la organizații în care aveți încredere: banca, organizațiile guvernamentale sau internaționale.
- Insistența de a ocoli sau a ignora politicile sau procedurile de securitate ori o ofertă care sună prea bine ca să fie adevărată (din păcate chiar nu ați câștigat la loterie).
- Un mesaj care pare să vină de la un prieten sau un coleg, dar semnătura, formulările sau tonul mesajului nu seamănă cu stilul cunoscut.

Până la urmă, cea mai bună apărare împotriva acestor atacuri sunteți dvs.

2 Home Network

Rețeaua de acasă: aproape fiecare rețea de acasă începe cu o rețea wireless (numit adesea Wi-Fi). Aceasta vă permite să vă conectați dispozitivele la internet. Majoritatea dispozitivelor wireless din casă sunt controlate de routerul internet sau de un punct de acces wireless separat. Cele două aparate funcționează la fel: transmit semnale wireless la care se conectează dispozitivele din casă. Acest lucru înseamnă că securizarea rețelei wireless este o componentă esențială a apărării casei. Vă recomandăm să luați următoarele măsuri pentru a vă apăra căminul:

- Schimbați parola implicită de administrator pe aparatul care controlează rețeaua wireless. Contul de administrator este cel cu care puteți configura setările rețelei wireless.
- Asigurați-vă că la rețea se pot conecta numai oameni în care aveți încredere. Acest lucru se obține prin activarea securității stricte. Dacă activați această opțiune, oamenii se vor putea conecta la rețea numai dacă știu parola, iar odată conectați, activitățile lor online vor fi criptate.
- Asigurați-vă că parola cu care utilizatorii se conectează la rețeaua wireless este una puternică și că este diferită de parola de administrator. Nu uitați că parola se introduce o singură dată în fiecare dispozitiv, întrucât acesta o păstrează și o refolosește.

Nu știți cum să luați aceste măsuri? Întrebați furnizorul de servicii internet, căutați pe site-ul acestuia, consultați documentația pe care ați primit-o cu punctul de acces wireless sau consultați site-ul producătorului.

3 Passwords

Parolele: atunci când un site vă solicită să creați o parola, creați una puternică. Cu cât are mai multe caractere, cu atât este mai puternică în fața atacurilor. Utilizarea unei fraze de acces este una dintre cele mai simple metode de a crea o parolă puternică. Fraza de acces nu este altceva decât o parolă alcătuită din mai multe cuvinte, de exemplu, „*fotoliu struguri cafea*”. Utilizarea frazelor de acces unice înseamnă să aveți câte una diferită pentru fiecare dispozitiv sau cont online. Astfel, dacă o frază de acces este compromisă, celelalte conturi și dispozitive rămân neafectate. Nu puteți reține toate frazele de acces?

Utilizați un manager de parole: acesta este un program special, care păstrează toate frazele acces într-un format criptat (și are multe alte funcții utile). Apoi,

activați verificarea în doi pași, numită și autentificare cu doi factori, dacă este posibil. Aceasta folosește parola, dar adaugă un al doilea pas, cum ar fi un cod trimis la smartphone sau o aplicație care generează codul. Este probabil ca verificarea în doi pași să fie cea mai importantă măsură pe care o puteți lua pentru a vă proteja conturile online și se folosește mult mai ușor decât ați crede.



Actualizări: aveți grijă ca toate computerele, dispozitivele mobile, programele și aplicațiile să aibă cea mai recentă versiune de software. Infractorii cibernetici caută mereu noi vulnerabilități în software-ul pe care îl folosiți. Atunci când le găsesc, folosesc programe speciale pentru a le exploata și pentru a vă sparge dispozitivele. Între timp, companiile care au creat software-ul acestor dispozitive lucrează din greu la corectarea vulnerabilităților prin lansarea de actualizări. Dacă aveți grijă ca aceste actualizări să fie instalate rapid pe computere și pe dispozitivele mobile, hackerilor o să le fie mult mai greu să vă atace. Pentru a avea mereu versiunea actuală, activați actualizarea automată ori de câte ori acest lucru este posibil. Regula este valabilă pentru aproape orice echipament conectat la o rețea, nu doar pentru dispozitivele cu care lucrați: televizoare conectate la internet, camerele de urmărire a bebelușilor, camerele de supraveghere, routerele din casă, consolele de joc și chiar mașina.



Copii/invitați: la birou nu se pune problema ca membrii familiei, copiii sau invitații să vă folosească laptopul de serviciu sau alte dispozitive cu care lucrați. Asigurați-vă că toată familia și toți prietenii înțeleg că nu vă pot folosi dispozitivele de lucru, pentru că pot șterge sau modifica din greșeală informații sau, mai rău, pot infecta dispozitivul.