[FRONTCOVER]

[Start Community Language Document 1]

Cyber aware

(Conștientizarea cibernetică)

Centrul Național de Securitate Cibernetică – ediția pentru formate alternative.

Acest conținut a fost produs de către Lead Scotland împreună cu partenerii săi și cu finanțare din partea Unității de Reziliență Cibernetică a Guvernului Scoțian.

Prezentul ghid are la bază conținutul disponibil pe site-ul web al Centrului Național de Securitate Cibernetică.

Informațiile au fost împărțite în 7 documente în limbi comunitare care sunt:

- Prezentul document, care include o Introducere și o prezentare a 6 Măsuri pe care le puteți lua pentru a îmbunătăți securitatea dumneavoastră online.
- Documente individuale detaliate pentru cele 6 Măsuri pe care le puteți lua.
- Toate link-urile menționate pot fi accesate vizitând site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/.

6 modalități de a îmbunătăți securitatea online

Datorită Coronavirusului, oamenii petrec anul acesta mai mult timp online.

Acest lucru înseamnă mai multe oportunități pentru hackeri de a realiza atacuri cibernetice. Deseori realizează acest lucru prin vizarea oamenilor și afacerilor folosind:

- E-mail-uri și camere web.
- Malware–este un software care vă poate deteriora dispozitivul sau care poate lăsa hackerul să pătrundă în dispozitiv.

Dacă hackerii intră în dispozitivul sau conturile dumneavoastră, vor putea avea acces la banii dvs., la informațiile personale sau la informații privind afacerea dvs.

Puteți îmbunătăți securitatea dvs. cibernetică luând 6 măsuri:

Măsura 1 –Folosiți o parolă puternică, separată, pentru e-mail.

Măsura 2 –Creați parole puternice folosind 3 cuvinte la

întâmplare.

Măsura 3 –Salvați parola în browserul dvs.

Măsura 4 –Porniți autentificarea cu doi factori (2FA).

Măsura 5 –Actualizați-vă dispozitivele.

Măsura 6 –Faceți o copie de rezervă a datelor.

[End Community Language Document 1]

[Start Community Language Document 2]

MĂSURA 1 – Folosiți o parolă puternică, separată, pentru email

Dacă un hacker intră în email-ul dumneavoastră, vă poate reseta celelalte parole de conturi și poate accesa informații salvate cu privire la dvs. sau la afacerea dvs.

Parola de email trebuie să fie puternică și diferită de celelalte parole. Acest lucru va îngreuna spargerea sau ghicirea ei.

Folosirea a trei cuvinte la întâmplare este o metodă bună de a crea o parolă puternică, unică, pe care să o țineți minte. Vom detalia acest lucru în următorul document.

De asemenea, trebuie să vă protejați și celelalte conturi importante, precum cel bancar sau de social media.

De ce este email-ul atât de important?

Email-ul este unul dintre conturile dvs. cele mai importante. Dar de ce le pasă hackerilor de email-urile dumneavoastră?

Imaginați-vă că un hacker vă intră în email

Acum poate accesa informații pe care le-ați salvat cu privire la

dvs. sau la persoanele de contact și poate pretinde că sunteți dvs.

Dar cel mai rău este că vă poate bloca accesul la conturile dvs. online.

Poate face acest lucru accesând oricare dintre conturile dvs. și folosind caracteristica „parolă uitată”.

Se va trimite astfel un email cu un link pentru a vă reseta

parola, iar hackerul îl poate folosi pentru a vă bloca accesul

la cont.

Odată ce a resetat o parolă, poate continua să reseteze parole și pentru celelalte conturi.

Prin urmare, cum vă puteți proteja email-ul și cum puteți ține hackerii la distanță de conturile online?

Folosiți o parolă puternică pentru email și asigurați-vă că este diferită de toate celelalte parole pe care le folosiți.

Asta înseamnă că dacă cineva vă sparge parola de la un alt cont, nu o va putea folosi pentru a intra în email.

Țineți minte, email-ul dvs. este unul dintre conturile dvs. cele mai importante. Asigurați-vă că este în siguranță.

Cum să vă schimbați parola de email

Cum să vă schimbați parola de la:

- Gmail.
- Yahoo!.
- Outlook.
- BT.
- AOL Mail.

Dacă email-ul dvs. nu este menționat aici, căutați online sfaturi de la furnizorul dvs. cu privire la modul în care vă puteți schimbați parola de email.

Sfaturi privind parolele pentru comercianții unici și micile afaceri

Dacă sunteți proprietar de afacere, conturile dvs. pot include informații sensibile cu privire la clienții, afacerea și finanțele dvs.

În cazul în care conturile dvs. nu sunt în siguranță, afacerea poate fi expusă riscului unui atac cibernetic. Acest lucru vă poate pune afacerea în pericol juridic sau financiar și în pericolul de a încălca Regulamentul General privind Protecția Datelor (GDPR).

Dacă afacerea dvs. are angajați, asigurați-vă că nu stochează parolele lângă dispozitivele lor și că acele dispozitive sunt blocate sau oprite atunci când nu sunt folosite.

Pentru mai multe informații, consultați Centrul Național de Securitate Cibernetică, Small Business Guide (Ghidul micilor afaceri).

Toaste link-urile menționate pot fi accesate vizitând site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 2]

[Start Community Language Document 3]

MĂSURA 2 Creați parole puternice folosind trei cuvinte la întâmplare

Atunci când folosiți parole puternice pentru conturile importante, poate fi dificil să vi le amintiți pe toate.

O metodă bună de a crea parole puternice, memorabile, este de a folosi trei cuvinte la întâmplare.

Nu folosiți cuvinte care pot fi ghicite (precum numele animalului dvs. de companie). La nevoie, puteți include numere și simboluri. De exemplu: RedPantsTree4! (RoșuPantaloniCopac4!)

Salvarea parolelor în browserul dvs. vă va ajuta să le gestionați; vom detalia acest lucru în documentul următor.

Testați-vă cunoștințele pentru a crea parole puternice

Puteți ghici care dintre următoarele parole nu apare în topul 100.000 cele mai compromise parole?

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- RedPantsTree
- Victoria!
- 2011977

Răspunsul este RedPantsTree.

Hackerii distribuie online liste care conțin milioane de parole compromise.

3 cuvinte la întâmplare este o metodă mai ușoară de a crea parole noi care sunt mai probabile de a fi unice și mai puțin probabile de a fi ghicite.

Toate link-urile menționate pot fi accesate prin vizitarea site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 3]

[Start Community Language Document 4]

MĂSURA 3 Salvați-vă parolele în browser

Salvarea parolelor în browser înseamnă să permiteți browserului dvs. web (precum Chrome, Safari sau Edge) să vă memoreze parolele.

Acest lucru vă poate ajuta să:

- Vă asigurați că nu vă pierdeți sau uitați parolele.
- Vă poate proteja împotriva unor delicte cibernetice precum site-urile web false.

Este mai sigur decât să folosiți parole slabe sau aceeași parolă în mai multe locuri.

Asigurați-vă că vă protejați parolele salvate în caz că vă pierdeți dispozitivul sau este furat.

Cum să vă protejați parolele salvate

Cineva care are acces la dispozitivul dvs. poate folosi parolele dvs. salvate pentru a vă accesa conturile.

Acest tip de delict cibernetic este mai puțin obișnuit decât atacurile de la distanță prin intermediul internetului, unde parolele sunt sparte folosind un software specific.

Pentru a vă asigura că sunteți protejați, trebuie să:

- Opriți sau să vă blocați dispozitivul atunci când nu îl folosiți.
- Folosiți o parolă puternică pentru a vă proteja dispozitivul.
- Porniți autentificarea cu doi factori pentru toate dispozitivele și conturile dvs.
- Porniți biometria (recunoașterea prin identificare facială sau amprentă), în cazul în care dispozitivul dvs. acceptă acest lucru.

De asemenea, ar trebui să faceți o copie de rezervă a datelor în mod regulat. Acest lucru vă va ajuta să recuperați informațiile importante dacă vă pierdeți dispozitivul sau dacă este furat.

Cum să vă salvați parolele în browser

Aflați cum să vă salvați parolele în:

- Google Chrome.
- Microsoft Edge.
- Firefox.
- Safari.

Știați că?

Vă puteți accesa parolele salvate de pe orice dispozitiv în care sunteți conectați la același browser.

Adăugați protecție suplimentară

Odată ce ați setat parole puternice, separate (Măsurile 1 - 3) pentru toate dispozitivele și serviciile, mai sunt și alte lucruri pe care le puteți face pentru a reduce riscul de a fi piratat (Măsurile 4 - 6).

Toate link-urile pot fi accesate vizitând site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 4]

[Start Community Language Document 5]

MĂSURA 4 Porniți autentificarea cu doi factori (2FA)

Autentificarea cu doi factori (2FA) împiedică hackerii să intre în conturile voastre, chiar dacă au parola dvs.

Anumite software-uri de banking online folosesc 2FA în mod automat. Fac acest lucru solicitând mai multe informații pentru a vă verifica identitatea, cum ar fi un cod trimis către telefonul dvs.

Cum să porniți autentificarea cu doi factori (2FA)

Veți avea nevoie să porniți manual autentificarea 2FA pentru majoritatea conturilor dvs. Nu toate conturile pun la dispoziție 2FA. Software-urile de banking online folosesc 2FA în mod automat.

2FA mai este cunoscută și ca verificarea în doi pași sau autentificarea cu factori multipli.

VIDEO: Cum funcționează 2FA

Accesul la video-ul How 2FA works este disponibil pe YouTube.

Porniți 2FA pentru email

- Gmail.
- Yahoo.
- Outlook.
- AOL.

Porniți 2FA pentru social media

- Instagram.
- Facebook .
- Twitter.
- LinkedIn.

Toate linkurile menționate pot fi accesate vizitând site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 5]

[Start Community Language Document 6]

MĂSURA 5: Actualizați-vă dispozitivele

Software-urile, aplicațiile și sistemele de operare expirate au puncte slabe. Acest lucru le face mai ușor de piratat.

Companiile remediază punctele slabe prin lansarea de actualizări. Atunci când vă actualizați dispozitivele și software-urile, țineți la distanță hackerii.

Porniți actualizările automate pentru dispozitivele și software-urile dvs. care le oferă. Asta înseamnă că nu trebuie să vă amintiți să o faceți dvs.

Unele dispozitive și software-uri trebuie să fie actualizate manual. Puteți primi memento-uri pe telefon sau calculator. Nu le ignorați. Actualizarea vă va ajuta să le păstrați în siguranță în mediul online.

Cum să porniți actualizările automate

Aflați cum să porniți actualizările automate pentru:

- Apple - Mac
- Apple - iPhone și iPad
- Microsoft Windows 10. – Căutați actualizările pentru Windows 10
- Windows 7 nu mai este acceptat. Ar trebui să faceți upgrade la Windows 10
- Android smartphones și tablete
- Android apps

Întrebare: Cum remediază companiile punctele slabe în software-ul lor?

- Bandaj
- Patch
- Reparație

Răspuns: Atunci când o companie găsește un punct slab în software-ul său, lansează un 'patch' pentru a-l remedia. Acest lucru ajută la păstrarea informațiilor în siguranță.

Toate linkurile menționate pot fi accesate vizitând site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 6]

[Start Community Language Document 7]

MĂSURA 6 – Faceți copie de rezervă a datelor

Copia de rezervă înseamnă să creați o copie a informațiilor dvs. și să o salvați pe un alt dispozitiv sau pe spațiul de stocare cloud online.

Creând cu regularitate copii de rezervă înseamnă că veți avea mereu o versiune recentă a informațiilor salvate. Acest lucru vă ajută să recuperați rapid datele pierdute sau furate.

De asemenea, puteți porni realizarea automată a copiei de rezervă. Vă va salva cu regularitate informațiile în stocarea cloud, fără să fiți nevoiți să țineți minte.

Dacă faceți copii de rezervă pe un stick USB sau un hard drive extern, deconectați-l de la calculator atunci când nu faceți copii de rezervă.

Știați că?

Trebuie să creați mereu copii de rezervă ale datelor înainte de

actualizarea dispozitivului. Explicația este că uneori actualizările pot

să înlăture sau să modifice fișiere.

Cum să porniți realizarea automată a copiei de rezervă

Cum să porniți realizarea automată a copiei de rezervă pentru:

- Apple – Mac.
- Apple - iPhone și iPad.
- Android.
- Microsoft Windows 10 și Windows 8 OneDrive.

Sfaturi cu privire la copiile de rezervă pentru comercianții unici și micile afaceri

Realizarea de copii de rezervă ale datelor înseamnă că afacerea dvs. poate continua să funcționeze dacă are loc un incident cibernetic.

Începeți prin identificarea datelor care sunt cele mai importante pentru afacerea dvs. Ele pot fi financiare, contractuale, legate de clienți sau furnizori. Asigurați-vă că le faceți cu regularitate copii de rezervă.

Trebuie, de asemenea, să știți cum să restabiliți o copie de rezervă în eventualitatea pierderii datelor.

Pentru mai multe informații, accesați Centrul Național de Securitate Cibernetică Small Business Guide (Ghidul micilor afaceri)

Toate linkurile menționate pot fi accesate vizitând site-ul web al Centrului Național de Securitate Cibernetică la adresa https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document7]

[END OF DOCUMENT