

OUCH!

Buletin informativ lunar pe teme de securitate pentru dvs.

# Curățenia de primăvară

## Prezentare generală

Cei mai mulți dintre noi așteptăm primăvara cu nerăbdare! Peisajul începe să se contureze, florile încep să înflorească și, pentru mulți, există dorința de a face curățenia de primăvară. În timp ce nevoia de a curăța și de a face ordine poate părea evidentă, nu se poate spune același lucru și despre curățenia digitală. Iată câteva sfaturi rapide pentru a vă pune în ordine viața digitală și pentru a stabili noi obiceiuri digitale:



**COPII DIGITALE DE REZERVĂ:** Enumerăm acest prim pas pentru că, pe termen lung, este unul din cele mai importante și e bine să îl faceți înainte de a trece la altele. Oricât de în siguranță și protejați ați fi, la un moment dat veți avea nevoie de copii digitale de rezervă(backup) pentru a recupera informații importante. Motivele pot include defecțiuni ale hard disk-ului, pierderea unui dispozitiv și infectarea cu un program tip malware cum ar fi virusii ransomware. Crearea și programarea automată a copiilor de rezervă va asigura posibilitatea de recuperare a celor mai importante informații pentru dvs.



**ȘTERGEREA:** Ștergeți orice program de pe calculator sau aplicație mobilă pe care nu le folosiți. Unele aplicații necesită mult spațiu de stocare, pot introduce noi vulnerabilități sau pot încetini dispozitivele folosite. Cu cât aveți mai puține aplicații cu atât sistemul și informațiile dvs. vor fi mai în siguranță. Multe dispozitive arată cât timp a trecut de când nu ați folosit o aplicație-dacă au trecut mai multe luni, este posibil să nu aveți nevoie de acea aplicație!



**ACTUALIZARE:** Actualizați-vă toate dispozitivele și aplicațiile și permiteți actualizarea automată ori de câte ori este posibil. Astfel, dispozitivele și aplicațiile rămân actualizate, au o viteză mai bună de procesare și devin mai greu de atacat.



**PAROLE:** Verificați-vă parolele. Dacă folosiți aceeași parolă pentru mai multe conturi, schimbați-le astfel încât fiecare cont să aibă o parolă unică. Nu vă puteți aminti toate parolele unice? Luați în considerare utilizarea unui administrator de parole. În ultimul rând, activați autentificarea cu doi factori(2FA) ori de câte ori este posibil, în special pentru conturile de email sau financiare.



**CONTURI FINANCIARE:** Asigurați-vă că aveți activate alertele pentru conturi bancare, cărți de credit sau fonduri de pensie, pentru a fi notificați de fiecare dată când o tranzacție este efectuată, în special pentru achiziții considerabile și transferuri de bani. Cu cât observați mai repede o activitate frauduloasă cu atât mai repede o puteți opri. În funcție de țara în care locuiți, înghețarea liniei de credit poate fi una din cele mai eficiente modalități de a vă proteja identitatea.



**NAVIGATORUL:** Verificați toate programele de completare (gen add-on și plugin) instalate în navigatorul dvs. Verificați setările legate de permisiuni; au aceste programe nevoie să vă acceseze locația, parolele și listele de contacte? Dacă nu mai folosiți anumite programe de completare și aveți temeri legate de confidențialitate, ștergeți-le.



**REȚELE DE SOCIALIZARE:** Verificați-vă prezența online și luați-o în stăpânire. Analizați-vă setările de confidențialitate și ștergeți pozele sau videoclipurile care nu mai sunt accesate sau necesare. De asemenea, vă puteți căuta numele prin intermediul motoarelor de căutare pentru a vedea ce informații există despre dvs. Nu uitați, e bine să limitați cantitatea de informații împărtășite cât și persoanele cărora doriți să le transmiteți informația.



**BIROUL:** Faceți ordine în sertarele biroului, ștergeți unități de stocare a datelor mai vechi (hard drive și memorii USB) și distrugeți notițele adezive cu prea multe informații. Puteți investi într-un distrugător de documente dacă nu aveți deja unul.



**EMAIL:** Curățați fișierele de email, ștergeți ce este nefolositor și organizați fișierele de care aveți nevoie. Acordați o atenție deosebită documentelor cu informații sensibile, cum ar fi data nașterii sau codul numeric personal, e bine să le ștergeți din inbox!

Deși poate părea o sarcină grea, fiți siguri că dispozitivele și informațiile dvs. vor fi mult mai protejate. Dacă pare a fi prea mult, puteți alege doar câteva articole sau puteți verifica doar un articol pe zi sau pe săptămână. Fiecare măsură, oricât de mică, vă va asigura mai multă protecție.

## Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Alflați mai multe la: <https://www.ubisoft.com/en-us/>

## Editor invitat

**Katie Nickels (@LiketheCoins)** este analist principal de informații, lucrează pentru Red Canary și este instructor SANS pentru FOR578: Serviciul de informații împotriva atacurilor cibernetice. Katie are peste 10 ani de experiență în securitatea rețelelor, intervenție în cazul incidentelor de securitate și inteligența informației împotriva atacurilor cibernetice.



## Resurse

Aveți backup?

<http://www.sans.org/u/ZVr>

Soluții pentru problema parolelor:

<http://www.sans.org/u/Y63>

Căutați-vă prezența online:

<http://www.sans.org/u/ZVB>

Scăpați de dispozitive mobile vechi:

<http://www.sans.org/u/ZVG>

OUCH! este publicat de SANS Security Awareness și este distribuit sub licența [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Puteți să partajați sau să distribuiți acest buletin informativ, cu condiția să nu îl vindeți și să nu îl modificați. Comitetul editorial: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tradus de: Oana Elena Cucu