G DATA press release 2016

G DATA Password Manager face ordine in jungla parolelor

G DATA Total Protection cu noul Password Manager asigura mai multa securitate pe Internet.

Bucuresti (Romania) 17.08.2016

O parola pentru fiecare - conturi de e-mail, conturi de social media, smartphone-uri, ATM-uri, magazine online. Acest lucru apasa pe umerii multor persoane. Conform unui studiu realizat de agentia digitala Bitkom, 36% dintre germani se simt coplesiti de numarul de parole. Un manager de parole ajuta la organizarea numeroaselor parole si, in acelasi timp, asigura mai multa securitate. Un modul Password Manager, usor de utilizat, a fost integrat in G DATA Total Protection. Functia cripteaza datele sensibile, cum ar fi numele de utilizator si parolele, intr-o baza de date de pe hard disk.

Noul modul G DATA Password Manager memoreaza parolele pentru magazine online, forumuri si conturi de e-mail. Password Manager apare ca o pictograma in browser, la instalare si, daca este cazul, salveaza fiecare parola necesara pentru site-urile utilizate pentru accesarea conturilor criptate. Datele sunt criptate si stocate pe hard disk si doar utilizatorul poate avea acces la aceste date, folosind o parola master. Integrarea acestui modulul reprezinta sfarsitul parolelor nesigure si a notitelor de pe fituici de hartie.

Expertul G DATA in securitatea datelor, Tim Berghoff, cantareste argumentele pro si contra parolelor in intrarea sa de pe blog si ofera patru sfaturi pentru securizarea conturilor. El pledeaza in special impotriva folosirii aceleasi parole pentru mai multe conturi: "Motivul este simplu. Daca parola utilizata pentru securizarea contului de e-mail sau a retelelor sociale este furata, un atacator are acces la identitatea voastra online. Acest lucru este ca si cum ati pierde o cheie universala care se potriveste la toate yalele usilor locuintei voastre."

Sfaturi de securitate de la G DATA

- *Verificati* pe site-uri web, cum ar fi https://www.leakedsource.com sau https://haveibeenpwned.com, daca adresa voastra de e-mail sau numele de utilizator apar in rezultatele cautarii. In cazul in care apar, nu intrati in panica. Asta nu inseamna neaparat ca cineva a abuzat de conturile voastre de utilizator. Cu toate acestea, modificati parola in cauza sau stergeti imediat contul respectiv daca acesta nu mai este utilizat.

- *Instalati un manager de parole*. Principiul este extrem de simplu: generati o parola puternica si suficient de complexa, care indeplineste toate cerintele, dar care nu trebuie sa fie memorata - programul va face asta in locul vostru. G DATA include un modul Password Manager in noua versiune a solutiei Total Protection. Dupa instalare, apare ca o pictograma in browser si ia cunostinta de fiecare parola de pe site-urile pe care aveti acces la conturi protejate prin parola.

- *Creati o prezentare generala* si, daca este necesar, schimbati parolele. Pentru a incepe crearea unei imagini de ansamblu, poate fi de ajutor sa alcatuiti o lista cu toate conturile si parolele asociate pe o coala de hartie, nu pe computer. In cazul in care este evident faptul ca aceeasi parola este utilizata pentru mai multe conturi de utilizator, schimbati toate parolele. Totusi, schimbarea parolelor nu inseamna adaugarea unor numere consecutive, de genul *Parola1*, *Parola2*, etc. Ganditi-va la o noua parola sau generati una folosind managerul de parole.

- *Aplicati autentificarea 2-factor* in cazul in care este posibil. Optiunile corespunzatoare sunt numite in mod uzual "a doua faza a conectarii", "confirmare Login" sau similar. Facebook, LinkedIn, Dropbox, Google, PayPal si o serie de alti furnizori importanti de servicii ofera aceasta optiune.

Mai multe informatii gasiti pe blogul G DATA https://blog.gdatasoftware.com/2016/28917-p-55w0rd5-blessing-or-curse

-###-