

Titel Bølge af afpresningsmails med adgangskoder

Brødtekst

Der er aktuelt en bølge af afpresninger i gang, hvor IT-kriminelle sender emails, hvor de har angivet en valid emailadresse samt en adgangskode, som har været anvendt.

Af Ricci Setholm

Ofte vil afpresseren påstå at have overtaget brugerens webcam, som jo anvendes betragteligt mere i disse tider, og har optaget videoer, som de vil dele på sociale medier, hvis der ikke betales en løsesum. Der har ikke været eksempler på, at dette er korrekt i nogen tilfælde. Såfremt du er i tvivl, skal du kontakte din lokale politimyndighed.

Oplysningerne som sendes til modtageren er fra en database på internettet, hvor der er brugernavn og adgangskoder fra tidligere hacks af større internet-baserede services. Blandt disse services er eksempelvis Adobe, LinkedIn og Sony, hvor særligt sidstnævnte er med logins til Playstation Network. Det er selve systemerne hos disse leverandører, som er hacket, og så er brugernavne, adgangskoder og lignende udtrukket på millioner af brugerkonti.

Som bekendt er det vigtigt, at du ikke anvender den samme adgangskode til flere steder, eksempelvis må du ikke anvende din Vestforbrænding adgangskode til andre systemer eller hjemmesider. Yderligere skal du huske at skifte dine adgangskoder.

Du kan selv som privatperson undersøge om din email-adresse (særligt din private) og en tidligere adgangskode er til salg, ved at indtaste dine anvendte email adresser på denne hjemmeside: <https://haveibeenpwned.com/>

Understående er et eksempel på, at min private email-adresse er til salg – Jeg har selvfølgelig skiftet mine adgangskoder 😊

ricci@setholm.dk pwned?

Oh no — pwned!
Pwned on 7 breached sites and found no pwns (subscribe to search sensitive breaches)

3 Steps to better security [Get using 1Password](#)

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.
Compromised data: Email addresses, Password hints, Passwords, Usernames

Data Enrichment Exposure From PDK Customer: In October 2015, security researchers Venny Trois and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index including a file was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDK, and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the wild following the release of the data.
Compromised data: Email addresses, Passwords

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HOP by a source who requested it to be attributed to "BenjaminDuke@exploit.in".
Compromised data: Email addresses, IP addresses, Passwords, Usernames

Udløber 01-01-2100

Afsender Økonomi & IT

Skrevet 14-04-2020

Oprettet kl. 14-04-2020 13:39 af Agnes Jantzen Kreinøe (AJK)
Sidst ændret kl. 14-04-2020 13:39 af Agnes Jantzen Kreinøe (AJK)

Luk