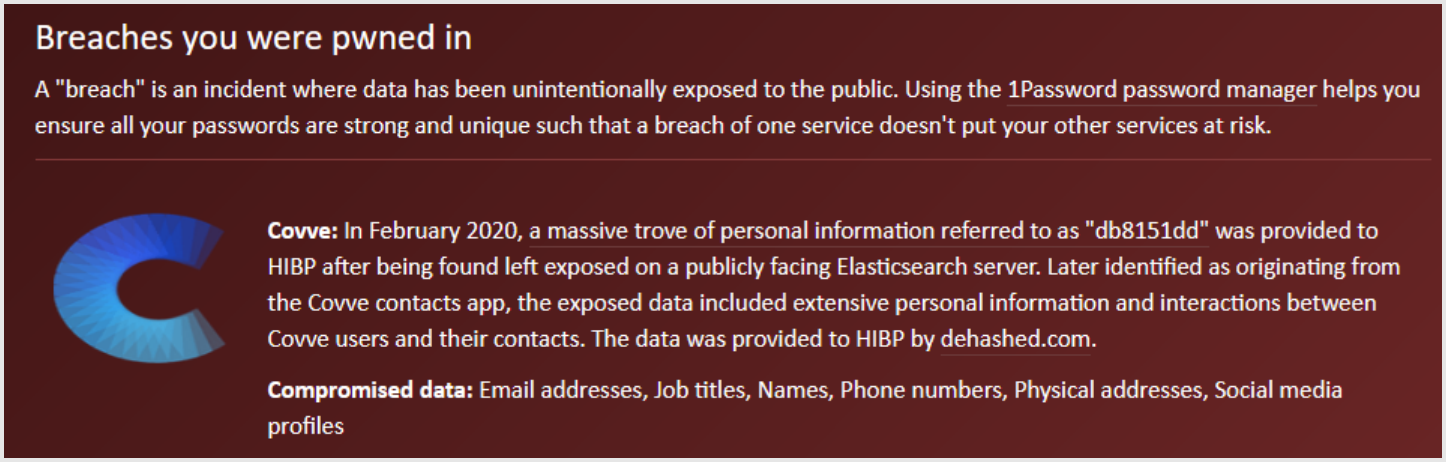
“Have I been pwned”?

Ako je Vaša e-adresa pronađena na stranici “Have i been pwned” (https://haveibeenpwned.com/; HIBP), to znači da je netko neovlašteno ušao u neki sustav (ali ne Vaš, nego sustav nekog teleoperatera, nekog portala, e-mail servera i sl) i došao do podataka korisnika tog servera (e-adresa, lozinka, broj telefona, …). Ne možemo se zaštititi od takvih vrsta “provale” i sve ovisi isključivo o vještini i količini novaca i vremena koji su dani na raspolaganje ljudima koji čuvaju podatke na serverima i onima koji napadaju te servere.

Skeniranje računala i zaštita računala ESET-ovim programom nisu nikako povezani s činjenicom da je Vaša e-adresa izlistana na HIBP.

Na toj istoj stranici (HIBP) se može ponekad i vidjeti u kojim napadima su Vaši podaci došli u ruke onima kojima nisu bili namijenjeni. Uzmimo za primjer rezultat za jednu od naših e-adresa koju koristimo za testiranja:



Tako su u spomenutom napadu napadači došli do e-adresa, funkcija osoba, njihovih imena, brojeva telefona, adresa stanovanja i podataka o profilima na socijalnim medijima. U našem konkretnom slučaju – za testne adrese koristimo izmišljene podatke i nije nam zabrinjavajuće što netko neželjen sada ima te informacije o nama. No, može biti zabrinjavajuće nekome tko je ostavio stvarne podatke, stoga dajemo nekoliko jednostavnih pravila za “ponašanje” na Internetu koje vrijedi za sve situacije i za sve usluge:

- Za svaku online uslugu upotrijebite novu lozinku
- (Ako je moguće koristite svaki puta drugu e-adresu, no ovo je danas teško izvedivo u praksi jer svi inzistiraju na tome da prijavite i broj telefona kada kreirate novu e-adresu)
- Bilo bi odlično koristiti:
    - jednu e-adresu za privatnu komunikaciju
    - drugu e-adresu za poslovnu
    - treću adresu za prijave na razne stranice na internetu
- Lozinka uopće ne mora biti “komplicirana” (osim ako na tom serveru inzistiraju na tome); važno je da bude što duža – npr. ova lozinka je vrlo sigurna i lako se pamti
- `Lozinka uopće ne mora biti "komplicirana"`
- Povremeno promijenite lozinke; ako je lozinka dugačka kao u gornjem primjeru dovoljno ju je promijeniti jednom godišnje; kraće lozinke mijenjajte češće
- Što Vam je važnija usluga – to duže lozinke koristite i češće ih mijenjajte
- Ako je omogućeno – koristite dvočlanu autentikaciju (2FA; v.ESA)

- Pokazat će se potreba i za korisštenjem nekog programa za upravljanje lozinkama (PWM; v.ESSP)
- Ako nije neophodno za funkcionalnost usluge koju namjeravate koristiti – ne ostavljajte svoje stvarne podatke (ime, prezime, broj telefona, adresu i slično) na serverima

---