Krypto-IT

Poradnik bezpiecznego korzystania z komputera i internetu od Krypto-IT.

Mówi się, że każdy człowiek powinien mieć swojego prawnika i księgową. W dzisiejszych czasach warto dodać do tego własnego informatyka!

Łącząc się do otwartej sieci Wi-Fi (lub takiej, której nie ufamy do końca) używajmy VPNów w celu uniknięcia podsłuchania tego, co wysyłamy do i ściągamy z internetu,

- sieć otwarta to taka do której mamy dostęp bez hasła,
- niektóre sieci zamknięte (zabezpieczone hasłem) powinniśmy również traktować jako niezaufane,
- do niezaufanych sieci należy dodać sieci hotelowe, schroniskowe i wszystkie do których o hasło wystarczy spytać.

Unikajmy otwierania nieznanych załączników i wchodzenia na podejrzane strony,

- jak otrzymamy wiadomość której się nie spodziewamy, założmy podstęp socjotechniczny,
- jeżeli w takiej wiadomości jest załącznik - załóżmy że to może być wirus,
- wchodząc na link w takiej wiadomości, możemy pobrać wirusa,
- podawanie haseł oraz danych osobowych, nawet gdy jesteśmy o to zapytani w linku z mejla, to zły pomysł,
- dla pewności warto spytać swojego informatyka o opinię.

Do przechowywania haseł dobrze mieć sprawdzony menadżer haseł i pamiętać tylko jedno hasło dostępowe do reszty,

- jeżeli jednak potrzebujemy pamiętać hasło, po pierwsze zastanówmy się, czy na pewno?
- jeżeli jednak musimy mieć hasło które pamiętamy, wybierzmy je składając ciąg losowych słów i pisząc je razem (ew. zaczynając z wielkich liter każdy wyraz), możemy wtrącać też cyfry i znaki specjalne,
- hasło typu: `UstawaRegulujeOpodatkowaniePodatkiem` jest długie, łatwo wpisać, ale wyrazy nie są losowe - lepiej wybrać coś na zasadzie: `GzegzolkaOrazRozowyOpodatkowanyOrzel`.

Jeżeli prowadzimy jakąkolwiek korespondencję przez internet - pamiętamy, że nie można mieć 100% że to na pewno osoba która się przedstawia - szczególnie jeżeli nie jest to wideo-konferencja,

- czaty tekstowe, korespondecja poczty elektronicznej - tam gdzie jest tylko tekst powinny być mniej zaufane dla zasady,
- rozmowy głosowe i wideo-konferencje można traktować jako najbardziej zaufane,
- najważniejsze wiadomości e-mail można podpisywać cyfrowo - to umożliwia potwierdzenie nadawcy,
- dla uzyskania obszerniejszej infomacji o podpisywaniy mejli warto spytać swojego informatyka.

Najważniejsze pliki warto mieć skopiowane na co najmniej jeden dysk zewnętrzny, ewentualnie pendrive,

- darmowe chmury obliczenieniowe i ich witualne dyski, nie są do końca dobrym pomysłem - firmy dostarczające te usługi zarabiają na reklamach, więc część plików może być skanowana przez automaty,
- jak komputer ulega awarii, a terminy gonią, warto mieć kopię tak przygotowaną, żeby można było na innym, zaufanym komputerze kontynuować pracę.

Warto szyfrować dyski z najważniejszymi danymi,

- do zaszyfrowanych plików nie dostaniemy się bez hasła,
- niektóre systemy szyfrowania dysków wysyłają hasła do chmury - to nie jest polecane rozwiązanie,
- szyfrowanie nieznacznie spowalnia używanie plików, głównie na początku, potem komputer się „rozpędza",
- jest parę dobrze sprawdzonych i polecanych systemów szyforwania dysków,
- dobrze spytać swojego informatyka o więcej szczegółów.

Posiadajmy aktualne oprogramowanie,

- wraz z aktualizacjamy ściągane są poprawki do programów. Bez nich może ktoś się do nas po prostu włamać,
- dodatkowo niektóre aktualizacje przyspieszają komputer.

Wszędzie, gdzie się da - używajmy szyfrowanych połączeń

- https zamiast http,
- pop3s, imaps, smtps, ... zamiast pop3, imap, smtp,
- jeżeli nie mamy pewności - spytajmy swojego informatyka.

Tam, gdzie jest to możliwe - warto używać uwierzytelnienia dwuskładnikowego, nazywanego również uwierzytelnieniem wieloskładnikowym

- możemy do tego wykorzystać specjalną aplikację na smartphone, czy wiadomość SMS
- inną możliwością jest specjalny klucz USB który jest uważany za najbezpieczniejsze rozwiązanie
- taka forma logowania wymaga oprócz znania hasła do konta tego drugiego mechanizmu
- z uwierzytelnieniem dwuskładnikowym nawet kiedy ktoś pozna hasło - nie daje to możliwości zalogowania
- w przypadku zabezpieczenia kluczem USB warto mieć 2 na wypadek zgubienia jednego

Bądźmy świadomymi użytkownikami sieci internet

- nie bójmy się pytać informatyków o pomoc, czy poradę
- nie ignorujmy ostrzeżeń, przestróg czy porad które mają pomóc nam się ochronić w sieci
- weryfikujmy to co widzimy w przeglądarce zamiast ufać bezgranicznie temu, co się wyświetla
- w internecie jest dużo śmieci, podpuch i innych pułapek - nie dajmy się tym zagrożeniom
- im więcej będzie świadomych użytkowników, tym działalność przestępcza będzie mniej opłacalna