Pierwsze internetowe łącze analogowe w Polsce zostało uruchomione 26 września 1990 r. Od tego czasu sporo się zmieniło, a internet stał się nieodłączną częścią naszego życia - odpisujemy na Messengerze, robimy zakupy przez Allegro, zamawiamy jedzenie, płacimy rachunki, oglądamy seriale na Netflixie, wrzucamy zdjęcia na Instagrama. Szczególnie w dobie Covid19, nauka oraz praca odbywa się zdalnie. Korzystając z sieci powinniśmy jednak zachować ostrożność, gdyż brak "cyfrowej higieny" może doprowadzić do katastrofy. Z okazji Dnia Bezpiecznego Internetu, przedstawiamy 10 porad jak bezpieczniej korzystać z internetu:

**1. Używaj silnych haseł**

Hasło powinno być odpowiednio długie, niepowtarzalne oraz niezawierające bezpośrednich powiązań z tobą (np. data urodzenia). Jeśli masz z tym problem, lub łapiesz się na korzystaniu z tego samego hasła w wielu miejscach, skorzystaj z menadżerów haseł, takich jak chociażby Dashlane czy KeePass.

**2. Korzystaj z uwierzytelniania dwuskładnikowego**

Jeśli to tylko możliwe, włącz uwierzytelnianie dwuetapowe (np. sms z kodem) w serwisach, z których korzystasz. Dzięki temu osoba trzecia znająca twoje hasło nie będzie mogła zalogować się bez podania kodu z sms przychodzącego na twój telefon.

**3. Uważaj na oszustwa**

Dokonując transakcji online jesteśmy narażeni na oszustwa. Przykładem mogą być fałszywe sklepy kusząco niską ceną i szybką dostawą. Staraj się korzystać z popularnych, oficjalnych sklepów. Jeśli dokonujesz transakcji przez portal aukcyjny / ogłoszeniowy, staraj się weryfikować rzetelność sprzedawcy np. czy nie wysłał towaru niskiej jakości lub innego niż deklarowano (np. chleb krojony zamiast telefonu). Aby stwierdzić, czy sprzedawca jest uczciwy możemy kierować się szczegółowymi, pozytywnymi opiniami; ilością sprzedanych dóbr lub datą założenia konta. Jeśli zostałeś oszukany, a za towar płaciłeś kartą, możesz spróbować cofnąć transakcję korzystając z procedury chargeback.

**4. Pamiętaj o aktualizacjach**

Ludzie tworzący oprogramowanie popełniają błędy, a błędy da się wykorzystywać w złych celach. Pamiętaj więc o aktualizacjach oprogramowania z którego korzystasz, szczególnie takiego jak system operacyjny czy przeglądarka. Dzięki temu eliminujesz niepotrzebne ryzyko

**5. Zwracaj uwagę na to, co udostępniasz**

Przed publikacją zdjęcia czy wiadomości, zwróć uwagę na jej treść. Z pozoru niewinne zdjęcie biletu lotniczego na selfie z lotniska, zdjęcie polubione przez twoją mamę, czy pesel może stanowić furtkę dla przestępców. Dane takie jak imię panieńskie matki, pesel, numer telefonu, data urodzenia, zdjęcie dowodu może zostać wykorzystane np. do wzięcia tak zwanej “chwilówki” lub do podszywania się przed operatorem naszej sieci telefonicznej (dzięki temu przestępca ma kontrolę nad kodami SMS potwierdzającymi logowanie lub resetowanie hasła).

**6. Strzeż się przed phishingiem**

Spróbuj wyobrazić sobie sytuację, że pewnego dnia otrzymujesz email od twojego banku o treści “twoje oszczędności zostały zablokowane, z powodu podejrzenia o wspieranie terroryzmu, aby odblokować swoje oszczędności, musisz przejść przez specjalną procedurę weryfikacji dostępną pod linkiem twójbank.pl/procedura”. Wyglądem strona nie różni się niczym od dobrze ci znanej strony banku. W procedurze, musisz podać dane do weryfikacji takie jak dane osobowe, zdjęcie dowodu, imię panieńskie matki, numer telefonu, hasło. Następnie, całość musisz potwierdzić kodem, który przyjdzie na twój telefon. Przestępca jest już właśnie o krok od kradzieży wszystkich pieniędzy z twojego konta bankowego. Pamiętaj, że “nadawca” w mailu może zostać sfałszowany, a przestępca może kupić domenę łudząco podobną do twojej strony bankowej.

**7. Uważaj na fałszywe SMSy**

Pamiętaj, że nadawca sms może zostać łatwo sfałszowany. Szczególnie popularny scenariusz to “dopłata” za paczkę, gdzie link w wiadomości sms prowadzi do fałszywej strony, wyłudzającej nasze dane.

**8. Uważaj na złośliwe oprogramowanie**

Złośliwe oprogramowanie wykrada dane z naszego urządzenia np. komputera lub smartfona. Aby tego uniknąć, zastanów się dwa razy, zanim uruchomisz plik z nieznanego źródła. Szczególnie narażeni jesteśmy gdy korzystamy z pirackiego oprogramowania lub podróbek aplikacji mobilnych. Dlatego korzystaj z oryginalnego oprogramowania i weryfikuj pliki pochodzące z nieznanego źródła, korzystając np. z serwisu Virustotal.

**9. Nie bądź mułem finansowym**

Uważaj na oferty pracy kuszące szybkim zarobkiem za “pośredniczenie w transakcjach bankowych’. Jeśli ktoś poprosi Cię o transfer pieniędzy za pośrednictwem konta bankowego w zamian za gotówkę, to prawdopodobnie nakłania cię do pomocy w procederze prania brudnych pieniędzy.

**10. Myśl za innych**

W internecie tak jak w ruchu drogowym, musisz myśleć nie tylko za siebie, ale i za innych. Informuj innych o zagrożeniach. Szczególnie narażone są osoby starsze np. rodzice.

Pamiętaj że wszelkie incydenty możesz zgłosić na incydent.cert.pl - jest to zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w Internecie.