Bądź CyberOdporny!

Poznaj haki na cyberataki

INSTYTUT KOŚCIUSZKI

Santander Fundacja

Bezpieczeństwo haseł

1. Nie używaj prostych oraz oczywistych haseł!

Chociaż pokusa jest spora, nie warto używać bardzo łatwych do odgadnięcia haseł typu „hasło", „admin" lub swojego imienia, nazwiska czy daty urodzenia. Proste kombinacje liczbowe typu 123456 także nie są dobrym pomysłem. Hakerzy posiadają bazy danych w których znajdują się setki tysięcy podobnych, najczęściej używanych, haseł – oznacza to, że będą w stanie złamać twoje proste hasło w kilka sekund! Wniosek: im bardziej skomplikowane i dłuższe, tym lepsze!

2. Jedno dobre hasło to za mało!

Nie ustawiaj tego samego hasła, nawet jeśli jest dobre i skomplikowane, do twoich wszystkich kont. Szczególnie groźne jest posiadanie jednego hasła do mediów społecznościowych, bankowości, serwisów aukcyjnych oraz poczty elektronicznej. Wyciek takiego hasła może Cię kosztować dostęp do wszystkich serwisów w jednym momencie.

3. Regularnie zmieniaj hasła!

Zmieniaj hasła regularnie, nie zapominaj o tym ważnym kroku!

4. Uważaj gdzie zapisujesz hasło!

Pulpit lub jakikolwiek folder na dysku twojego komputera nie jest bezpiecznym miejscem na zapisanie swoich haseł, szczególnie jeśli użyjesz do tego pliku tekstowego. Podobnie z popularną możliwością zapisania haseł w przeglądarce, jest to bardzo wygodna opcja jednak nie do końca bezpieczna. Szyfrowanie w przeglądarkach nie zapewnia pełnego bezpieczeństwa, zapisywanie haseł za jego pośrednictwem jest więc sporym ryzykiem.

5. Używaj menedżera haseł!

Postępując zgodnie ze wszystkimi wytycznymi bezpieczeństwa będziesz posiadał kilkanaście skomplikowanych haseł, które bardzo trudno zapamiętać. Jest jednak rozwiązanie tego problemu, użyj sprawdzonego menedżera haseł, który pozwala na ich bezpieczne zapisanie. Dzięki niemu za pomocą jednego hasła zablokujesz dostęp do swoich wszystkich kont.

6. Uwierzytelnianie dwuskładnikowe!

Pozwala na dodatkowy element weryfikacji w procesie dostępu do twojego konta. Nawet jeśli twoje hasło znajdzie się w nieodpowiednich rękach to dostęp do twojego konta z nowego urządzenia będzie wymagał potwierdzenia za pomocą smsa lub poczty internetowej.

Zakupy online

Zakupy w Internecie stały się już powszechne, a każdy z nas robi to przynajmniej kilka razy w miesiącu. Według badania GEMIUS i Izby Gospodarki Elektronicznej już 73% internautów robi zakupy online. Poza wygodą i dostępem do szerokiego asortymentu, ten rodzaj handlu niesie ze sobą pewne zagrożenia. Jak się przed nimi bronić?

1. Kupując w Internecie warto uważać na fałszywe witryny sklepowe - podstawową czynnością która może nas uchronić przed kosztowną pomyłką jest zwrócenie uwagi na szyfrowanie strony. Warto sprawdzić czy w pasku adresu w przeglądarce znajduje się ikona kłódki, a w następnym kroku czy certyfikat jest nadal ważny oraz dla kogo został wystawiony.

2. Warto zweryfikować dane firmy - adres, opinie on-line i wybierać tylko te sprawdzone.

3. Płacić za zakupy powinniśmy tylko poprzez znanego nam operatora, stosując uwierzytelnianie dwuskładnikowe.

4. Unikajmy tworzenia kont na sklepach internetowych, których nie znamy, bo mogą być to próby wyłudzeń haseł bądź kart kredytowych, zwłaszcza, jeżeli okazje na nich są „zbyt dobre, aby były prawdziwe".

5. Róbmy zakupy z poziomu oficjalnej strony sprzedawcy.

6. Publiczne sieci wi-fi, np. w kawiarniach czy bibliotekach, nie powinny być używane do robienia zakupów online.

Fałszywe strony internetowe

1. Na co uważać?

Manipulacja emocjonalna – za jej pomocą atakujący próbują zmylić twoją czujność.

- Pilna sprawa – oszuści używają ofert lub alertów które mają być ważne tylko przez krótki okres czasu i które wymagają natychmiastowego działania.
- Podekscytowanie – atrakcyjne oferty, karty podarunkowe czy darmowe prezenty mają zwrócić twoją uwagę, a ich atrakcyjność przykryć potencjalne podejrzane elementy oferty.
- Strach – agresywne komunikaty o zainfekowaniu twojego komputera mają sprawić że będziesz działał w panice.

2. Jak zidentyfikować fałszywe strony?

1. Używają emocjonalnego języka
2. Amatorski wygląd strony
3. Niepoprawna gramatyka, składnia itp.
4. Brak informacji kontaktowych czy treści informacyjnych

3. Jak unikać fałszywych stron?

1. Sprawdź dokładnie adres strony – fałszywki używają często bardzo podobnych adresów do ich rzeczywistych odpowiedników, zmieniając jeden znak lub przestawiając ich kolejność.
2. Płać jedynie za pomocą sprawdzonych metod – czerwona lampka powinna się zaświecić w przypadku możliwości zapłaty jedynie za pomocą przelewu bankowego lub przez zewnętrzne i nieznane aplikacje.
3. Zbyt dobre, żeby było prawdziwe – oferty które są zbyt atrakcyjne muszą wzbudzić w nas nieufność.
4. Przeprowadź mini-śledztwo – jeśli masz jakiekolwiek podejrzenia, sprawdź daną stronę za pomocą popularnych wyszukiwarek, przeczytaj opinie oraz recenzję produktów.

Fałszywe linki i SMS, czyli *phishing*

Phishing jest rodzajem oszustwa, którego skuteczność opiera się na założeniu, że odbiorca np. SMS lub wiadomości e-Mail zachowa się w określony sposób, np. kliknie w link, udzieli wrażliwej informacji lub roześle dalej.

Jak zauważyć *phishing*?

1. E-mail został wysłany z publicznej domeny (np. @gmail.com) zamiast z konta firmowego,
2. Domena z której został wysłany mail zawiera błąd, np. @satnanderbankpolska.pl
3. Treść maila jest słabej jakości - niepoprawnie sformułowana, z błędami językowymi,
4. Zawiera nietypowe załączniki lub linki,
5. Prosi nas o podanie hasła lub danych do karty,
6. Tytuł lub treść maila nas ponagla lub próbuje emocjonalnie skłonić nas do jakiegoś działania.

Zabezpieczenie telefonu lub komputera

Aby zabezpieczyć się przed oszustwami i atakami:

1. Używaj oficjalnych i zaufanych aplikacji,
2. Korzystaj z antywirusa,
3. Nie zostawiaj haseł na wierzchu, nie podawaj ich osobom trzecim,
4. Aktualizuj system oraz bazę wirusów,
5. Nie używaj ogólnodostępnych sieci.

Poza powyższymi warto zainstalować śledzenie urządzenia (np. telefonu), żeby w razie zagubienia móc zlokalizować urządzenie. Przydatnym rozwiązaniem jest także ograniczenie dostępu do danych aplikacjom, które naszym zdaniem go nie potrzebują.