

# European Cyber Security Month

## Bezpieczeństwo finansowe w Internecie

6

wskazówek



### Upewnij się, że robiąc zakupy online, korzystasz ze sprawdzonych i bezpiecznych stron internetowych

1

Sprawdź, czy strona internetowa ma adres zaczynający się od https i zwracaj uwagę na błędy ortograficzne i gramatyczne. Przejrzyj stronę „O nas” i / lub „Skontaktuj się z nami”, aby upewnić się, że sprzedawca podaje prawdziwe dane kontaktowe. Uważaj na „niepowtarzalne okazje” i zapoznaj się z opiniami osób, które korzystały ze strony.



### Nigdy nie płać za zakupy kartą kredytową, korzystając z publicznej sieci Wi-Fi

2

Korzystając z publicznego połączenia Wi-Fi, nie masz pewności, że sieć jest odpowiednio zabezpieczona. Poczekaj, aż będziesz mógł połączyć się z bezpieczną siecią, zanim podasz np. numer konta bankowego. Jeśli nie możesz czekać, skorzystaj z połączenia VPN lub wyłącz Wi-Fi i połącz się przez swoje dane komórkowe.



### Wybieraj silne hasła

3

Wybór łatwych do zapamiętania haseł ułatwia cyberprzestępcom ich odgadnięcie. Upewnij się, że Twoje hasła są silne i nie używaj tego samego hasła do różnych kont. Oprogramowanie do zarządzania hasłami (menedżer haseł) może pomóc Ci w zarządzaniu wieloma złożonymi hasłami. Nigdy nie zostawiaj hasła na karteczce samoprzylepnej na komputerze!



### Bądź podejrzliwy w stosunku do pilnych wiadomości SMS, e-mail lub rozmów telefonicznych, które rzekomo pochodzą z Twojego banku lub innej instytucji

4

Jeśli wiadomość e-mail jest nieoczekiwana, oznaczona jako pilna i / lub wymaga natychmiastowego działania, prawdopodobnie jest fałszywa. Oszuści wzywają do natychmiastowego działania, aby zaskoczyć ludzi i skłonić ich do udostępnienia swoich danych osobowych. Nie reaguj! Nie spiesz się. Zweryfikuj prośbę bezpośrednio w banku lub innej instytucji.



### Bądź bardzo podejrzliwy wobec wszelkich wiadomości SMS lub e-mail, w których ktoś pisze, że ma dla Ciebie pieniądze

5

SMS lub e-mail obiecujący nieoczekiwany przyływ gotówki zawsze przyciągnie naszą uwagę. Niestety, zazwyczaj jest to oszustwo, ZWŁASZCZA jeśli ktoś wymaga od Ciebie wysłania pieniędzy lub danych osobowych, aby ją odebrać! Zignoruj informację o niespodziewanym szczęściu – jest oszustwo.



### Uważaj na oszustwa w mediach społecznościowych

6

Cyberprzestępcy wykorzystują różne oszustwa w mediach społecznościowych, aby uzyskać dostęp do Twoich informacji lub pieniędzy! Mogą ukrywać się za wiadomościami o „bezpłatnym okresie próbnym”, zaproszeniami od znajomych i pozornie niewinnymi quizami. A jeśli na Twojej stronie lub profilu w mediach społecznościowych pojawi się nietypowy link, nie klikaj go! Bo może on prowadzić do witryny wydłużającej informacje.