Czerwiec z bankiem spółdzielczym - IV tydzień

22.06.2020

Tematem przewodnim czwartego tygodnia jest:

"Edukacja w zakresie cyberbezpieczeństwa". Dzisiaj internetowy dostęp do konta bankowego stał się standardem w bankowości. Wraz z rozwojem usług bankowych pojawiają się nowe zagrożenia, gdyż przestępcy swoją aktywność przenoszą do cyberprzestrzeni. Dlatego też banki na całym świecie nieustannie pracują nad udoskonalaniem systemów zabezpieczeń. Rozwiązania, które oferują klientom muszą spełniać najwyższe wymogi bezpieczeństwa. Poniżej zamieszczamy materiały, które mamy nadzieję, iż pomogą poznać tajniki bezpiecznego poruszania się w bankowości internetowej oraz w sieci.

- Zasady bezpiecznego korzystania z usług bankowości.
- Poradnik "Zadbaj o swoje bezpieczeństwo w Internecie" czyli korzystać ze sprzętu komputerowego, na którym wykonuje się operacje w systemie bankowości internetowej.
- Malware to złośliwe oprogramowanie oprogramowaniem, zainstalowane w celu uzyskania dostępu do komputera bądź urządzenia mobilnego bez wiedzy jego użytkownika. Instalacja malware służy najczęściej pozyskaniu danych osobowych lub haseł do bankowości elektronicznej, co może następnie prowadzić do kradzieży pieniędzy z konta.

Jak unikać zagrożenia?
- używać programów antywirusowych, programów antymalware’owych, filtrów antyspamowych,
- nie otwierać załączników z e-maili nadesłanych z nieznanych adresów,
- zawsze instalować tylko oryginalne oprogramowanie, pochodzące z legalnego źródła,
- jeśli mamy podejrzenie, że komputer nie działa jak dotychczas, lepiej nie korzystać na nim z bankowości elektronicznej.

- Pharming to rodzaj oszustwa polegający na tym, że odwiedzający prawdziwą stronę banku są przekierowywani na podszywające się pod nią strony. Zanim jednak nastąpi faktyczne przekierowanie, przestępcy różnymi metodami instalują złośliwe oprogramowanie na komputerze lub urządzeniach z nim powiązanych np. routerze. To właśnie ten wirus przekierowuje ze strony, z której chcemy skorzystać np. strony banku na fałszywą stronę, która imituję tą, którą chcieliśmy otworzyć.

Jak unikać zagrożenia?
- zawsze zwracać uwagę na adres strony internetowej, na której wprowadzane jakiekolwiek dane,
- sprawdzić czy przed adresem jest skrót https oraz prawidłowa nazwa organizacji, która jest właścicielem strony, w szczególności zwracając uwagę na literówki w nazwie lub dodatkowe rozszerzenia,
- unikać podejrzanych stron i nigdy nie klikać w linki w e-mailach od osób, których nie znamy.

- ALERTY BIKWzmożona aktywność w internecie to także więcej okazji dla cyberprzestępców, którzy mogą wykraść Twoje dane i wykorzystać je do wyłudzenia kredytu czy zakupów na Twoje konto.
Czy wiesz, że aż 51% Polaków nie zna żadnych usług, które pomagają chronić dane osobowe? Ty także znajdujesz się w tej grupie? Nie daj się zaskoczyć!
Poznaj Alerty BIK – usługę, która poinformuje Cię o próbie wykorzystania skradzionych danych do wyłudzenia kredytu.

Polecamy nagranie wideo na temat cyberbezpieczeństwa:

- Odc. 1 Bądź cyberbezpieczny zawsze: Odc. 1 - Cyberbezpieczeństwo zaczyna się w domu https://www.youtube.com/watch?v=PcOIAApjFKA&feature=youtu.be
- Odc. 2 Bądź cyberbezpieczny zawsze:Odc. 2 - Cyberbezpieczeństwo w miejscu pracyhttps://www.youtube.com/watch?v=8ipYD-B9_UQ

Źródło: Warszawski Instytut Bankowości