Cyberbezpieczeństwo
– gdy złodziej czai się po drugiej stronie monitora, a nie za drzwiami.

Z CYBERBEZPIECZEŃSTWEM NA „TY”

Staramy się dbać o nasz dom poprzez regularne sprzątanie, ubezpieczenie wartościowych rzeczy i chcemy czuć się bezpiecznie zamykając go na klucz. Dobrze jest też pamiętać, że nasze wirtualne życie również zasługuje na zapewnienie odpowiedniej ochrony.

Na co dzień korzystamy z takich urządzeń jak bankomat, komputer lub telefon, które ułatwiają nam robienie zakupów, opłacanie rachunków lub kontrolę nad finansami, dlatego warto pamiętać o zasadach, które umożliwią zabezpieczenie tego, na co tak długo pracowaliśmy.

Ważne zasady, których przestrzeganie pozwoli zadbać o bezpieczeństwo Twoich finansów:

- hasła do kont powinny być unikatowe. Warto korzystać z małych i dużych liter a także cyfr i znaków specjalnych takich jak np. !, ?, #,
- nikomu nie udostępniaj swoich haseł lub PIN-ów oraz nie pozostawiaj ich w widocznym i łatwo dostępnym miejscu,
- zabezpiecz swoje urządzenia elektroniczne takie jak komputer, laptop, tablet czy telefon w bieżąco aktualizowane programy antywirusowe, które blokują dostęp wirusów do twoich urządzeń i chronią je przed utratą danych,
- dbaj o aktualizację oprogramowania systemowego i pozostałych programów na Twoim komputerze, tablecie i telefonie, by zabezpieczyć się przed wykrytymi błędami i korzystać z najbardziej aktualnych mechanizmów ochronnych,
- zwróć szczególną uwagę na strony www. Powinny być one zabezpieczone w formie kłódeczki, https://
- otrzymałeś wiadomość sms, na komunikatorze, w mediach społecznościowych lub pocztą elektroniczną, która wygląda podejrzanie np. nie jest pisana poprawną polszczyzną lub obiecuje wysoką nagrodę w zamian za pomoc? Nie odpowiadaj na nią i najlepiej od razu ją usuń,
- bądź szczególnie wyczulony na wiadomości z instytucji finansowych zawierające nietypowe prośby (np. o wpłatę środków) lub informacje z nieznanych Ci instytucji z prośbą o przesłanie pieniędzy lub numeru Twojego rachunku lub danych Twojej karty płatniczej to może być podstęp,
- pamiętaj, aby zawsze po załatwieniu wszystkich spraw wylogować się z systemu transakcyjnego oraz programu, z którego korzystasz,
- wystrzegaj się przekazywania swoich danych (numerów dokumentu tożsamości, PESEL, numeru konta, numeru karty płatniczej, kodu CVV itp.) poprzez media społecznościowe, komunikatory lub za pomocą poczty elektronicznej.

SKOK zależy na zapewnieniu bezpieczeństwa finansowego swoim członkom. Pracownicy SKOK z chęcią pomogą lub wyjaśnią w jaki sposób bezpiecznie korzystać z udostępnianych narzędzi, takich jak karta płatnicza czy bankowość internetowa (eskok) lub mobilna (mskok), tak abyś czuł się bezpieczny w cyber przestrzeni.

Stowarzyszenie Krzewienia Edukacji Finansowej