NARODOWY BANK POLSKI

DOBRE PRAKTYKI CYBERBEZPIECZEŃSTWA

Nie podawaj nieznajomym swoich danych w internecie. Nie są tam bezpieczne.

Korzystaj wyłącznie z zabezpieczonych i zaufanych sieci Wi-Fi, szczególnie przy przetwarzaniu ważnych informacji.

Nie otwieraj załączników i nie klikaj w linki w wiadomościach od nieznanych nadawców. Nierozważne działanie może spowodować, że stracisz dane osobiste lub pieniądze.

Nie ujawniaj innym osobom numerów PIN ani haseł do systemów. One nie lubią zmieniać właściciela.

Nie podłączaj do swojego komputera obcych dysków czy nośników USB. Mogą zainfekować Twój sprzęt, a właściciel może nie wiedzieć, że jego pendrive rozprzestrzenia wirusa.

Zainstaluj zaufane aplikacje zabezpieczające Twoje urządzenie komunikacyjne. Wiele fabrycznych zabezpieczeń wygasa po okresie próbnym.

Stosuj na telefonie zabezpieczający kod PIN lub inne silne zabezpieczenia.

Korzystaj z portali społecznościowych wyłącznie na swoich osobistych urządzeniach: smartfonie czy laptopie.

Używaj silnych haseł i je chroń. Co najmniej 12 znaków zawierających małe i wielkie litery, cyfry i symbole. Różne hasła wykorzystuj do różnych kont. Nigdy ich nikomu nie udostępniaj, ani adminom, ani nawet znajomym!

Nie udostępniaj nikomu swoich urządzeń komunikacyjnych: telefonu, laptopa czy tableta, i nie zostawiaj ich niezabezpieczonych w publicznych miejscach. One są tylko Twoje!

DOBRE PRAKTYKI CYBERBEZPIECZEŃSTWA

Poznaj zasady, jak być odpornym na socjotechnikę i oszustwa (deepfake, dezinformacja). Każdy może być „słabym ogniwem". Tylko edukacja może zminimalizować zagrożenie.

Nie publikuj informacji osobistych w mediach społecznościowych w myśl zasady, że „w Internecie nic nie ginie". Nie akceptuj zaproszeń od nieznanych osób. Konta w mediach społecznościowych traktuj jako prywatne.

Szanuj użytkowników Internetu, nie udostępniaj obraźliwych treści ani komentarzy. Pamiętaj, że wszystko, co publikujesz, może zostać zapisane i użyte w przyszłości.

Naucz się rozpoznawać zagrożenia takie jak phishing czy złośliwe oprogramowanie, aby chronić swoje wrażliwe dane np. dotyczące konta bankowego.

Chroń swoje numery PIN i numery kart płatniczych. Ich utrata może być kłopotliwa i bardzo kosztowna.

Rób kopie bezpieczeństwa swoich danych, zapisując je na dysku zewnętrznym lub w chmurze, gdzie regularnie są tworzone kopie bezpieczeństwa.

Dbaj o równowagę między aktywnościami online, a życiem poza Internetem, angażując się w sport, hobby czy spotkania ze znajomymi.

Stosuj na telefonie co najmniej kod PIN, aby chronić jego zasoby. Pamiętaj, że PIN może mieć więcej niż 4 znaki.

Nie podejmuj decyzji pod wpływem presji lub emocji. Zawsze przemyśl odpowiedzi na prośby o podanie wrażliwych danych (dane logowania, dane osobowe).

Jeśli zobaczysz coś podejrzanego, bądź padniesz ofiarą cyberprzemocy lub innego zagrożenia, nie wahaj sie szukać pomocy u rodziców, nauczycieli lub specjalistów.

Odświeżaj wiedzę z cyberbezpieczeństwa. Tu zmiany zachodzą nieustannie, ponieważ cyberprzestępcy wciąż doskonalą swoje metody działania.

Pamiętaj! Incydenty naruszające bezpieczeństwo w sieci zgłaszaj do Cert Polska. Zgłoś na stronie: **incydent.cert.pl**. Podejrzane wiadomości SMS prześlij pod numer: **8080**