CYBERBEZPIECZEŃSTWO

W celu podnoszenia świadomości w zakresie cyberbezpieczeństwa przedstawiamy informacje dotyczące najczęściej występujących zagrożeń w cyberprzestrzeni oraz podstawowych zasad bezpiecznego korzystania z Internetu, urządzeń elektronicznych i usług cyfrowych.

Cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub świadczonych usług.

Najczęstsze zagrożenia w cyberprzestrzeni

- **Phishing** – wyłudzanie danych osobowych, haseł lub pieniędzy poprzez podszywanie się pod zaufane osoby, firmy i instytucje, najczęściej za pomocą fałszywych wiadomości e-mail i stron internetowych.
- **Smishing** – oszustwa wykorzystujące wiadomości SMS, np. fałszywe informacje o przesyłkach, płatnościach lub konieczności aktualizacji danych.
- **Vishing** – próby wyłudzenia informacji lub pieniędzy podczas rozmów telefonicznych, często poprzez podszywanie się pod pracowników banków, urzędów lub innych instytucji.
- **Złośliwe oprogramowanie (malware)** – programy mogące powodować kradzież, uszkodzenie lub utratę danych.
- **Ransomware** – oprogramowanie blokujące dostęp do danych lub systemów, często połączone z żądaniem okupu.
- **Kradzież tożsamości** – bezprawne wykorzystanie danych osobowych innej osoby.
- **Przejęcie kont internetowych** – uzyskanie nieuprawnionego dostępu do poczty elektronicznej, bankowości internetowej lub innych usług.
- **Fałszywe strony internetowe i sklepy** – witryny tworzone w celu wyłudzenia danych osobowych lub pieniędzy.
- **Ataki socjotechniczne** – manipulowanie użytkownikami w celu nakłonienia ich do ujawnienia informacji, przekazania pieniędzy lub wykonania niebezpiecznych działań.

Jak chronić się przed cyberzagrożeniami?

1. **Aktualizuj oprogramowanie** – regularnie instaluj aktualizacje systemu operacyjnego, przeglądarki internetowej i aplikacji.
2. **Korzystaj z oprogramowania zabezpieczającego** – stosuj aktualną ochronę antywirusową i zaporę sieciową.
3. **Stosuj silne i unikalne hasła** – nie używaj tego samego hasła do różnych kont. Rozważ korzystanie z menedżera haseł.
4. **Włącz uwierzytelnianie wieloskładnikowe (MFA/2FA)** – szczególnie w przypadku poczty elektronicznej, bankowości i innych ważnych usług.
5. **Zachowaj ostrożność wobec wiadomości e-mail i SMS** – nie otwieraj podejrzanych linków ani załączników, nawet jeżeli wiadomość pochodzi od pozornie znanego nadawcy.
6. **Sprawdzaj adresy stron internetowych** – przed zalogowaniem się lub podaniem danych upewnij się, że korzystasz z właściwej strony. Samo połączenie HTTPS nie gwarantuje jej wiarygodności.
7. **Nie udostępniaj haseł ani kodów autoryzacyjnych** – nie przekazuj ich osobom kontaktującym się telefonicznie, e-mailem lub przez komunikatory.
8. **Korzystaj z zaufanych urządzeń i połączeń** – unikaj logowania do ważnych usług na urządzeniach publicznych i niezaufanych.
9. **Chroń dane osobowe** – nie przekazuj ich nieznanym osobom ani nie wprowadzaj na niesprawdzonych stronach internetowych.

10. **Wykonuj kopie zapasowe** – przechowuj kopie ważnych danych w bezpiecznym miejscu.
11. **Instaluj aplikacje z zaufanych źródeł** – unikaj nieznanego i nielegalnego oprogramowania.
12. **Zabezpieczaj urządzenia** – stosuj blokadę ekranu, hasło, PIN lub inne dostępne mechanizmy ochrony.
13. **Nie podejmuj pochopnych decyzji** – zachowaj szczególną ostrożność wobec wiadomości wywołujących presję czasu, strach lub obiecujących wyjątkowe korzyści.
14. **Reaguj na podejrzane zdarzenia** – w przypadku podejrzenia przejęcia konta, ujawnienia hasła lub infekcji urządzenia niezwłocznie podejmij działania zabezpieczające.

Gdzie zgłaszać cyberzagrożenia?

Podejrzane wiadomości, strony internetowe oraz incydenty cyberbezpieczeństwa można zgłaszać do CERT Polska:

- **Formularz zgłoszeniowy:** https://incydent.cert.pl
- **Podejrzane wiadomości SMS:** numer 8080 – wiadomość należy przekazać w oryginalnej formie.
- **Strona internetowa:** https://cert.pl

W przypadku podejrzenia oszustwa finansowego należy również niezwłocznie skontaktować się z bankiem, a w uzasadnionych przypadkach zawiadomić Policję.

Dodatkowe informacje

Więcej informacji i porad dotyczących bezpieczeństwa w Internecie można znaleźć na stronach:

- CERT Polska – https://cert.pl
- Poradniki CERT Polska – https://cert.pl/ouch/
- Ministerstwo Cyfryzacji – https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

Pamiętaj! Cyberbezpieczeństwo zależy nie tylko od stosowanych zabezpieczeń technicznych, ale również od wiedzy, ostrożności i odpowiedzialnego zachowania każdego użytkownika Internetu.