

Cyberbezpieczeństwo

W dzisiejszych czasach zagrożenia bezpieczeństwa informacji stanowią poważne wyzwanie dla każdej organizacji i indywidualnego użytkownika. Kradzież własności intelektualnej, wiadomości e-mail przesyłane przez cyberprzestępców oraz rozprzestrzenianie się złośliwego oprogramowania to realne problemy współczesnego świata. Cyberbezpieczeństwo to nie tylko temat dla specjalistów IT - to temat dla każdego z nas.

Nasza Spółka, utrzymując stały kontakt z klientami i partnerami biznesowymi za pośrednictwem elektronicznych kanałów komunikacji, przywiązuje szczególną wagę do bezpieczeństwa danych. Chcemy zapewnić Państwu dostęp do rzetelnej wiedzy na temat zagrożeń cyberbezpieczeństwa oraz praktycznych sposobów ochrony przed nimi.

Bezpieczeństwo w cyberprzestrzeni zależy przede wszystkim od świadomości i odpowiedzialności każdego użytkownika. Dlatego zachęcamy do zapoznania się z podstawowymi zasadami cyberbezpieczeństwa:

1. Nie otwieraj załączników z niezaufanych źródeł i nie klikaj w podejrzane linki. Chwila nieuwagi może spowodować, że staniesz się ofiarą cyberataku.
2. Sprawdzaj dokładnie adresy stron www – zwłaszcza tych, na których podajesz dane uwierzytelniające (login, hasło), szczególnie do elektronicznego Biura Obsługi Klienta czy usług bankowości elektronicznej.
3. W sposób regularny aktualizuj sprzęt i oprogramowanie, z którego korzystasz.
4. Nie podłączaj zewnętrznych nośników danych, jeśli nie jesteś pewny źródła ich pochodzenia.
5. Używaj haseł trudnych do odgadnięcia. Stosuj zasadę „jedno hasło do jednego konta”. Nie wykorzystuj tych samych haseł do logowania się w różnych serwisach i usługach.
6. Zanim klikniesz „OK”, przeczytaj uważnie, na co się zgadzasz.
7. Nie udostępniaj nikomu swoich danych uwierzytelniających (loginów, haseł).
8. Stosuj zasadę ograniczonego zaufania do publicznych sieci Wi-Fi. Podczas korzystania z nich nie używaj swoich danych uwierzytelniających (login, hasło).
9. Pamiętaj, że należy się wylogować ze swojego konta po zakończonej pracy z komputerem.
10. Dbaj o swoją prywatność. Odpowiednio ustawiaj zasady prywatności na portalach społecznościowych, świadomie decydując o tym, jakie informacje i w jaki sposób chcesz o sobie udostępniać.
11. Włączaj uwierzytelnianie dwuskładnikowe (2FA) wszędzie tam, gdzie jest ono dostępne. Dodatkowe zabezpieczenie znacznie utrudnia cyberprzestępcom dostęp do Twojego konta i Twoich danych.

Informacje dotyczące naruszenia zasad cyberbezpieczeństwa prosimy przesyłać na adres:

vpol.soc@veolia.com

Więcej aktualnych informacji na temat cyberbezpieczeństwa znajdziesz na stronie:

- Ministerstwa Cyfryzacji - <https://www.cyber.gov.pl/dla-obywatela>
- CSIRT GOV - <https://csirt.gov.pl/>