CYBERBEZPIECZEŃSTWO

1. Pamiętamy, że świadomość zagrożeń i odpowiednie działania są kluczowe dla bezpieczeństwa online naszych danych i urządzeń jak również dla organizacji, w której pracujemy.

2. Pamiętamy, aby regularnie aktualizować oprogramowanie użytkowe oraz systemy operacyjne używane w naszej organizacji.

3. Stosujemy się do zasad RODO - znamy swoje prawa i obowiązki wynikające z przepisów o ochronie danych osobowych.

3. Nie pozostawiajmy odblokowanych urządzeń bez nadzoru. Blokujemy dostęp, aby nikt niepowołany nie mógł z nich korzystać podczas naszej nieobecności.

4. Staramy się być ostrożni w mediach społecznościowych - uważamy, co udostępniamy online, gdyż może to być wykorzystane do stworzenia fałszywego profilu.

5. Korzystamy z bezpiecznych połączeń internetowych lub używajmy szyfrowanych połączeń VPN, podczas gdy łączymy się z ogólnodostępnymi nieznanymi sieciami bezprzewodowymi typu WI-FI (np. w hotelach, restauracjach, barach, itp.).

6. Zawsze korzystamy z oprogramowania antywirusowego i antyspamowego z automatyczną aktualizacją modułów antywirusowych oraz przynajmniej z zapory sieciowej firewall wbudowanej w system operacyjny.

7. Nie przekazujemy wrażliwych danych dotyczących pracowników lub organizacji w miejscach publicznych, w których przebywają osoby trzecie (np. na papierosie, w pociągu, itp.).

8. Stosujemy unikatowe hasła o odpowiednim poziomie skomplikowania (zawierające duże i małe litery, liczby, znaki specjalne, np.: #,$,!).

9. Nie podłączamy nieznanych urządzeń pamięci masowych do swojego komputera, np. znalezionego lub podarowanego przez kontrahenta pendrive'a, a także telefonów, dysków przenośnych etc.

10. Uważnie czytamy komunikaty i powiadomienia pojawiające się w trakcie logowania. Pamiętamy, że przestępcy potrafią podrabiać strony w Internecie. Zawiadamiamy dział IT, w przypadku gdy:

- zaskoczy nas coś w widoku strony www;
- odnotujemy nietypowe jej działanie;
- jest ona złudnie podobna do oryginalnych stron internetowych;
- nazwa strony internetowej zawiera błędy ortograficzne lub litery zlewają się w ciąg znaków podobnych do oryginalnych znaków stron www.

11. Uważamy na phishing, gdyż są to próby wyłudzenia od użytkowników ich danych osobowych i uprawnień do logowania do serwisów internetowych np. bankowości elektronicznej lub systemów informatycznych używanych przez naszą organizację. Najczęściej zagrożenie to posiada formę specjalnie spreparowanych wiadomości przesyłanych przez pocztę elektroniczną, które zgodnie z tą samą zasadą jak przy oszustwach ze stronami internetowymi, są złudnie podobne do oryginalnych adresów mailowych nadawcy i mogą zawierać błędy ortograficzne lub zlewać się w ciąg znaków podobnych do oryginalnych adresów mailowych.

12. Nigdy nie wysyłamy przez Internet przy pomocy sieci publicznej, niezaszyfrowanych danych wrażliwych, które mogą posłużyć do kradzieży tożsamości (PESEL, nr dowodu osobistego, itp.).

Phishing – *to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem, czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.*