CYBERBEZPIECZEŃSTWO, zgodnie z art. 2 pkt 4 ustawy *o krajowym systemie cyberbezpieczeństwa*, to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Ustawa *o krajowym systemie cyberbezpieczeństwa* zobowiązuje Szpital do zapewnienia użytkownikom usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych praktyk zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową (udzielanie świadczeń zdrowotnych).

Poniżej przedstawiamy najważniejsze informacje dotyczące najczęściej występujących cyberzagrożeń oraz sposoby ochrony przed nimi.

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

- ataki z użyciem szkodliwego oprogramowania (*malware*, wirusy, robaki itp. – szczegółowe informacje dotyczące zagrożeń technicznych znajdziesz **tutaj >>**);
- kradzieże tożsamości;

Co zrobić w przypadku kradzieży tożsamości? – szczegółowe informacje znajdziesz **tutaj >>** ;

Jak i gdzie zgłosić nieuprawnione wykorzystanie swoich danych osobowych (kradzież tożsamości)? – niezbędne informacje znajdziesz **tutaj >>** ;

- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych;
- blokowanie dostępu do usług;
- spam (niechciane lub niepotrzebne wiadomości elektroniczne);
- ataki socjotechniczne (np. *phishing*, czyli wyłudzanie poufnych informacji np. danych do logowania poprzez podszywanie się pod instytucję lub osobę godną zaufania, np. urzędy banki, znajomych, portale społecznościowe).

Podstawowym elementem bezpieczeństwa w sieci Internet jest zastosowanie zasady **ograniczonego zaufania i podwyższonej ostrożności**.

W celu ochrony przed zagrożeniami:

- Zabezpiecz dostęp do swojego komputera/urządzenia mobilnego hasłem lub innym bezpiecznym sposobem (jeśli masz taką możliwość np. odciskiem palca);
- Korzystaj wyłącznie z legalnego oprogramowania, pozyskanego z oficjalnego źródła – od producenta lub autoryzowanego dostawcy;
- Dbaj o regularne aktualizacje systemu operacyjnego i wszystkich zainstalowanych programów – to może Cię ustrzec przed szkodliwym oprogramowaniem i innymi zagrożeniami w sieci;
- Korzystaj z wbudowanej zapory sieciowej (firewall) oraz oprogramowania antywirusowego, które chroni sprzęt przed szkodliwymi programami, ale także zwiększa ochronę sieci oraz pozwala na filtrowanie stron internetowych pod kątem ich szkodliwości;
- Regularnie skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz, poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązuje własne połączenia z Internetem, wysyłając Twoje hasła i inne prywatne dane do sieci;

- Staraj się nie korzystać z sieci publicznych, jeżeli logujesz się do systemu/ aplikacji;
- Jeśli podłączasz do komputera nośniki danych – skanuj je pod kątem wirusów i złośliwego oprogramowania;
- Nie otwieraj podejrzanych załączników i nie klikaj w nietypowe linki – zwłaszcza te, pochodzące od nieznanych nadawców. Mogą zawierać szkodliwe oprogramowanie, które doprowadzi do utraty lub pozyskania Twoich danych (np. danych logowania do bankowości elektronicznej);
- Nie korzystaj ze stron internetowych (zwłaszcza stron banków, poczty elektronicznej), które nie mają ważnego certyfikatu (np. brak protokołu https) chyba, że masz pewność z innego źródła, że strona taka jest bezpieczna;
- Nie udostępniaj swoich danych osobowych w niesprawdzonych serwisach i na stronach internetowych, zawsze czytaj dokładnie Regulaminy i Polityki, weryfikuj na co wyrażasz zgodę;
- Nie wysyłaj e-mailem poufnych danych bez ich szyfrowania. Hasło do zaszyfrowanych przekazuj innym kanałem komunikacji niż dane;
- Pamiętaj, że Szpital, bank, czy urząd nie wysyła e-maili do swoich pacjentów/klientów/interesantów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji;
- Używaj silnych haseł, a jeśli to możliwe włącz uwierzytelnianie dwuskładnikowe;
- Nie udostępniaj nikomu swojego loginu i hasła;

Kompleksowy materiał dotyczący haseł znajdziesz **tutaj >>**

- Unikaj logowania do systemów/aplikacji z obcych urządzeń;
- Nie zapisuj haseł w pamięci przeglądarki;
- Wykonuj kopie zapasowe swoich danych;
- Zwracaj uwagę na komunikaty pojawiające się na ekranie i nigdy nie ignoruj ostrzeżeń dotyczących bezpieczeństwa;
- Jeżeli nie korzystasz w danej chwili z Wi-Fi lub Bluetooth, wyłącz je;
- Przed sprzedażą/oddaniem urządzenia innej osobie, usuń trwale z niego wszystkie dane.

Więcej informacji dla użytkowników komputerów na temat bezpieczeństwa można uzyskać na stronie zespołu reagowania na incydenty CERT Polska: https://www.cert.pl/ouch/

OUCH! to cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację.

Przeczytaj również:

Dla każdego – cyberhigiena

Informacje o oszustwach, których celem są polscy użytkownicy Internetu