Cyberbezpieczeństwo

Urząd Miasta Orzesze, zobowiązany został ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa do zapewnienia zainteresowanym stronom, wobec których świadczy zadanie publiczne zależne od systemu informacyjnego, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych praktyk zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami cyfrowymi.

W związku z powyższym przedstawiamy najważniejsze informacje dotyczące najczęściej występujących cyberzagrożeń oraz sposoby ochrony przed nimi.

Phishing – przestępcy tworzą fałszywe strony internetowe, żeby wyłudzić dane (loginy i hasła) użytkowników Internetu; w tym celu najczęściej wysyłają wiadomości e-mail zawierające odnośniki do tych stron. Jak się chronić? Dokładnie weryfikuj adresy stron WWW zanim się na nich zalogujesz. Nie wpisuj swojego loginu i hasła na podejrzanych stronach internetowych.

Malware/ ransomware – hakerzy często stosują ataki z użyciem szkodliwego oprogramowania (malware, ransomware itp.); mogą wysyłać złośliwe oprogramowanie za pośrednictwem wiadomości e-mail, dołączonego do e-maila załącznika. Jak się chronić? Nie otwieraj podejrzanych wiadomości oraz załączników, ponieważ w przypadku instalacji złośliwego oprogramowania na Twoim urządzeniu, hakerzy mogą przejąć dostęp np. do konta w Twoim banku.

Vishing – przestępcy mogą do Ciebie zadzwonić i podawać się za pracownika Urzędu lub innej instytucji (np. Policji) albo po prostu Twojego przełożonego i prosić Cię o przekazanie Twojego loginu, hasła, numeru PESEL, numeru dowodu osobistego; podanie tych danych może skutkować kradzieżą Twojej tożsamości, umożliwieniem przestępcy zalogowania się do systemu informatycznego Urzędu. Jak się chronić? Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz. Haseł do systemów informatycznych nie zdradzaj nigdy i nikomu.

Podstawowym elementem bezpieczeństwa w Internecie jest zastosowanie zasady ograniczonego zaufania i podwyższonej ostrożności. Dlatego też zachęcamy do:

- używania oprogramowania antywirusowego i zapory sieciowej (firewall);

- korzystania wyłącznie z legalnego i aktualnego oprogramowania;

- unikania korzystania z sieci publicznych, w przypadku logowania się do systemów informatycznych zawierających cenne dane lub dane podlegające ochronie;

- regularnej aktualizacji oprogramowania oraz bazy danych wirusów;

- nie otwierania podejrzanych e-maili oraz ich załączników;

- nie korzystania ze stron WWW, które nie mają ważnego certyfikatu (np. brak protokołu https);

- nie pozostawiania swoich danych osobowych w niesprawdzonych serwisach i na stronach internetowych;

- czytanie zawsze dokładnie Regulaminów i Polityk serwisów WWW oraz weryfikowanie zakresu wyrażanych zgód;

- nie wysyłania e-mailem poufnych danych bez ich szyfrowania;

Pamiętaj, że Urząd, bank, czy szpital nie wysyła e-maili do swoich pacjentów/klientów/interesantów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji!

Dodatkowe środki bezpieczeństwa w przypadku korzystania z systemów informatycznych oraz urządzeń mobilnych:

- blokuj ekran swojego urządzenia (np. hasło, PIN);

- włącz ustawienia blokady ekranu Twojego urządzenia;

- wpisując swoje hasło, pin, login zweryfikuj, czy nikt Cię nie nagrywa lub nie widzi tego, co wpisujesz;

- nie udostępniaj nikomu swojego loginu i hasła do systemu informatycznego;

- unikaj stosowania haseł, które można łatwo odgadnąć (np. poprzez powiązanie z Twoją osobą);

- hasło powinno mieć co najmniej 12 znaków w tym litery małe i duże, cyfry oraz znaki specjalne;

- nie zapisuj haseł na kartkach, w notatniku;

- stosuj różne hasła w różnych systemach informatycznych;

- unikaj logowania do systemów z cudzych urządzeń;

- nie zapisuj haseł w pamięci przeglądarki;

- przed sprzedażą / oddaniem urządzenia innej osobie, usuń z niego wszystkie dane;

- jeżeli masz taką możliwość korzystaj z nakładek prywatyzujących na monitor (również w urządzeniu mobilnym) w miejscach publicznych;

- pamiętaj o zainstalowaniu i aktualizacji systemów antywirusowych oraz ochrony sieciowej także w urządzeniach mobilnych;

- instaluj aktualizacje aplikacji i systemu operacyjnego w swoim urządzeniu mobilnym;

- pobieraj i instaluj aplikacje wyłącznie z oficjalnych sklepów z aplikacjami;

- nie uruchamiaj linków z wiadomości SMS lub e-mail, jeśli nie masz pewności, że pochodzą z bezpiecznego i zaufanego źródła;

- jeżeli nie korzystasz w danej chwili z Wi-Fi lub Bluetooth, wyłącz je.

Więcej informacji na stronie:

Portal Gov.pl – Baza wiedzy – Cyberbezpieczeństwo