# Powiatowe Centrum Pomocy Rodzinie w Krakowie

# Cyberbezpieczeństwo

Realizując obowiązek wynikający z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ( t.j. Dz.U. z 2020 r. poz. 1369) Powiatowe Centrum Pomocy Rodzinie w Krakowie przekazuje Państwu informacje pozwalające na lepsze zrozumienie zagrożeń cyberbezpieczeństwa oraz skuteczne sposoby zabezpieczania się przed tymi zagrożeniami.

**Co rozumiemy poprzez cyberbezpieczeństwo?**

Cyberbezpieczeństwo jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

**Co to jest incydent?**

Incydent jest to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

**Przykłady incydentów?**

Do najczęściej występujących incydentów należą:

- kradzież tożsamości,
- kradzież, modyfikacja lub niszczenie danych,
- działalność złośliwego oprogramowania (wirusów, trojanów, ransomeware itp.), które rozprzestrzenia się w postacie załączników do e-maili, linków w e-mailach lub na stronach internetowych,
- spam, czyli niechciane lub niepotrzebne wiadomości e-mail mogące rozprzestrzeniać złośliwe oprogramowanie,
- ataki socjotechniczne (np. phising, czyli wyłudzanie poufnych informacji poprzez podszywanie się pod godną zaufania osobę lub instytucję) w celu pozyskania np. danych logowania czy danych karty bankomatowej.

**Zabezpieczanie się przez tymi zagrożeniami:**

Najlepszym sposobem na ustrzeżenie się przed negatywnymi skutkami incydentów jest ochrona wcześniej zastosowana ochrona (ochrona prewencyjna) i dobre nawyki podczas korzystania z komputera, smartfona.

Niektóre z możliwych do zastosowania środków ochrony:

- zabezpieczenie systemu operacyjnego programem antywirusowym i zaporą sieciową (firewallem),
- skonfigurowanie programu antywirusowego, aby cały czas miał włączoną ochronę komputera, za każdym razem skanował podpinane nośniki cyfrowe np. pendrive i skanował pocztę elektroniczną,
- skonfigurowanie sporządzania kopii zapasowych danych,
- konfiguracja sieci bezprzewodowej aby co najmniej wymagała podania hasła do sieci.

Dobre nawyki:

- dbanie o aktualność systemu operacyjnego oraz oprogramowania antywirusowego – reagowanie na komunikaty

z tym związane,
- instalacja oprogramowania tylko z pewnego źródła np. strona producenta,
- sprawdzanie plików pobranych z internetu za pomocą programu antywirusowego,
- obserwowanie i czytanie komunikatów pojawiających się na ekranie komputera,
- unikanie odwiedzin stron zawierających darmowe pliki muzyczne, obrazy, filmy,
- jeśli to nie jest konieczne niekorzystanie z publicznych hot-spotów (dostępu do internetu) np. w kawiarniach, sklepach, na lotnisku, a już w szczególności jeżeli zamierzamy logować się do banku lub w inne ważne miejsce,
- sprawdzanie, czy strony internetowe w szczególności strony banków, platformy zakupowe posiadają ważny certyfikat bezpieczeństwa i połączenia są szyfrowane – należy zwrócić uwagę na zieloną kłódkę oraz na początek adresu czy jest tam „https”,
- niewysyłanie danych osobowych, logowania, numerów kont i kart kredytowych w niezabezpieczonych wiadomościach e-mail,
- uważne sprawdzanie odnośników, w które zamierza się kliknąć,
- weryfikacja adresu nadawcy wiadomości e-mail,
- konfiguracja filtrów antyspamowych dla e-maili,
- sprawdzanie czy wiadomość e-mail, tytuł tej wiadomości i nazwa załącznika mają sens,
- nieotwieranie maili jeśli są jakiekolwiek podejrzenia w powyżej wymienionym zakresie – usunąć bez otwierania,
- nieotwieranie załączników o rozszerzeniach *.exe, *.com, *.pif, *.scr, *.bat – może to być wirus,
- stosowanie silnych czyli haseł o długości min. 8 znaków składające się z wielkich i małych liter, cyfr i znaków specjalnych,
- używanie różnych haseł do różnych portali,
- nieużywanie w hasłach danych typu imię, nazwisko, data urodzenia lub popularnych słów,
- nieprzechowywanie haseł w widocznym miejscu (np. naklejonych na monitor, pod klawiaturą),
- w przypadku ujawnienia hasła natychmiastowa jego zmiana.

Należy pamiętać, że banki nigdy nie wysyłają w wiadomościach e-mail odnośników służących do potwierdzania haseł czy transakcji, weryfikacji danych konta ani próśb o zalogowanie się. Jeśli otrzymasz taką wiadomość, jak najszybciej zgłoś ten fakt obsłudze banku.

W celu uzyskania szczegółowych informacji dotyczących cyberbezpieczeństwa mogą Państwo odwiedzić strony internetowe Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo.