Powiat Kętrzyński

CUW
Centrum Usług Wspólnych
Powiatu Kętrzyńskiego

CYBERBEZPIECZEŃSTWO W PIGUŁCE

Dział IT Centrum Usług Wspólnych
Tel: 89 751 17 16

Opracował Piotr Krakowiak

Cyberbezpieczeństwa - dlaczego to takie ważne ?

W pracy urzędnika i nauczyciela masz dostęp do informacji, które są bardzo cenne — nie tylko dla instytucji, ale też dla cyberprzestępców. Są to m.in. dane osobowe uczniów, mieszkańców, dokumenty urzędowe czy dostęp do systemów administracyjnych.

Ataki coraz częściej są kierowane właśnie do instytucji publicznych i szkół, ponieważ:

- pracownicy otrzymują dużo maili i dokumentów,
- łatwo podszyć się pod „urzędowe pismo" lub „wiadomość ze szkoły",
- jeden błąd może dać dostęp do całego systemu.

Warto pamiętać: cyberprzestępca nie musi włamywać się do systemu — często wystarczy, że ktoś kliknie w złośliwy link lub poda hasło.

👉 **Dlatego Twoja ostrożność w codziennej pracy ma kluczowe znaczenie dla bezpieczeństwa całej instytucji.**

Hasła i dostęp do systemów

Hasło to podstawowa ochrona Twojego konta. Niestety, wiele incydentów wynika z używania prostych lub powtarzanych haseł.

Dobre praktyki:

- używaj różnych haseł do różnych systemów (np. poczta, dziennik, system kadrowy),
- twórz hasła o długości co najmniej 12 znaków,
- unikaj oczywistych słów (imię, nazwa szkoły, „123456").

Najlepiej stosować tzw. „hasła zdaniowe", np.:

„LubięPorannąKawę!2026"

Dodatkowo:

- jeśli to możliwe, włącz uwierzytelnianie dwuskładnikowe (2FA),
- nigdy nie udostępniaj swojego hasła innym osobom,
- nie zapisuj haseł na kartkach przy komputerze.

👉 **Jeśli masz podejrzenie, że hasło mogło wyciec — zmień je natychmiast.**

Fałszywe maile i wiadomości (phishing)

Phishing to jedna z najczęstszych metod ataku. Polega na podszywaniu się pod zaufane instytucje lub osoby, aby skłonić Cię do kliknięcia w link lub otwarcia załącznika.

Typowe przykłady:

- „Pilne pismo do zapoznania”
- „Faktura do opłacenia”
- „Zmiana hasła – kliknij tutaj”

Zwróć uwagę na:

- dziwny adres nadawcy (np. literówki w adresie e-mail),
- presję czasu („natychmiast”, „pilne”),
- podejrzane linki lub załączniki.

Nigdy:

- nie podawaj hasła przez e-mail,
- nie klikaj linków bez sprawdzenia,
- nie otwieraj załączników, jeśli nie masz pewności.

👉 **W razie wątpliwości — skontaktuj się z działem IT Centrum Usług Wspólnych.**

Załączniki i pliki

Załączniki to bardzo częsty sposób rozprzestrzeniania wirusów. Nawet jeśli wiadomość wygląda wiarygodnie, plik może zawierać złośliwe oprogramowanie.

Zasady bezpieczeństwa:

- otwieraj tylko pliki od znanych i zaufanych osób,
- zwracaj uwagę na rozszerzenia plików (np. .exe, .zip mogą być niebezpieczne),
- nie włączaj makr w dokumentach Office, jeśli nie wiesz, do czego służą.

Szczególnie niebezpieczne są:

- pliki „udające" dokumenty (np. faktura.pdf.exe),
- archiwa (.zip) z hasłem,
- nieoczekiwane załączniki od znajomych (ich konto mogło zostać przejęte).

👉 **Jeśli coś wzbudza Twoją wątpliwość — lepiej nie otwierać i skontaktować się z działem IT Centrum Usług Wspólnych.**

Sprzęt służbowy

Komputer służbowy powinien być używany wyłącznie do celów związanych z pracą. Instalowanie prywatnych programów lub korzystanie z nieznanych stron zwiększa ryzyko infekcji.

Pamiętaj:

- blokuj ekran, gdy odchodzisz od stanowiska (Win + L),
- nie udostępniaj swojego konta innym osobom,
- nie instaluj oprogramowania bez zgody działu IT.

Dodatkowo:

- nie podłączaj nieznanych pendrive'ów,
- przechowuj dokumenty tylko w zatwierdzonych lokalizacjach,
- dbaj o fizyczne bezpieczeństwo sprzętu (np. laptopa).

👉 **Twój komputer to „brama" do systemu — jego bezpieczeństwo ma ogromne znaczenie.**

Internet i praca zdalna

Podczas pracy zdalnej szczególnie ważne jest bezpieczne połączenie z internetem.

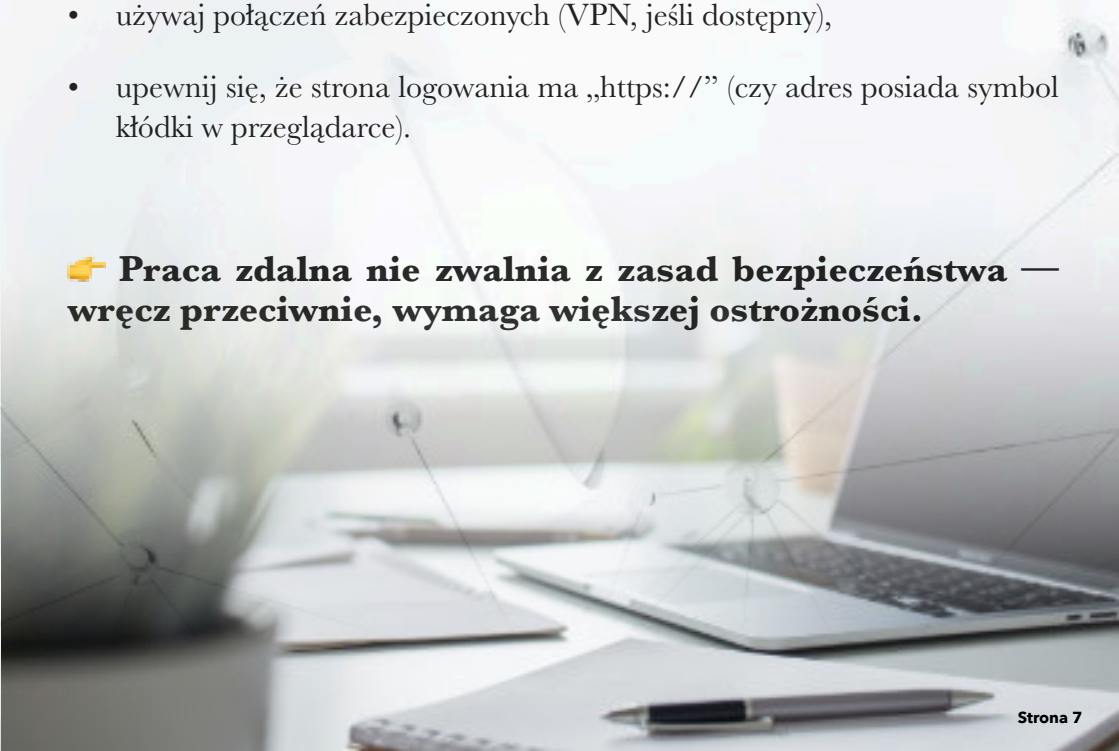
Unikaj:

- logowania do systemów służbowych przez publiczne Wi-Fi (np. w kawiarni),
- korzystania z prywatnej poczty do przesyłania dokumentów służbowych,
- instalowania nieautoryzowanych narzędzi.

Zalecenia:

- korzystaj tylko z oficjalnych systemów i aplikacji,
- używaj połączeń zabezpieczonych (VPN, jeśli dostępny),
- upewnij się, że strona logowania ma „https://" (czy adres posiada symbol kłódki w przeglądarce).

👉 **Praca zdalna nie zwalnia z zasad bezpieczeństwa — wręcz przeciwnie, wymaga większej ostrożności.**



Najważniejsze zasady i co zrobić w razie incydentu

W cyberbezpieczeństwie najważniejsze są codzienne nawyki oraz szybka reakcja, gdy coś pójdzie nie tak. Nie musisz być ekspertem IT — wystarczy stosować kilka podstawowych zasad.

Na co dzień pamiętaj:

- zawsze myśl zanim klikniesz w link lub załącznik,
- chroń swoje hasła i nie udostępniaj ich innym,
- dokładnie sprawdzaj nadawcę wiadomości,
- nie instaluj nieznanych programów ani aplikacji,

Mimo ostrożności może zdarzyć się sytuacja, która wzbudzi Twoje wątpliwości lub okaże się incydentem.

Jeśli:

- klikniesz podejrzany link, otworzysz nieznany załącznik,
- zauważysz nietypowe działanie komputera lub telefonu,

👉 **działaj natychmiast:**

- zgłoś sytuację do działu IT Centrum Usług Wspólnych
- jeśli to możliwe, odłącz urządzenie od internetu,
- zmień swoje hasła,

Nie próbuj ukrywać błędu — szybkie zgłoszenie pozwala ograniczyć skutki i chroni innych użytkowników.

👉 **Pamiętaj: w cyberbezpieczeństwie najważniejsza jest Twoja czujność i szybka reakcja.**