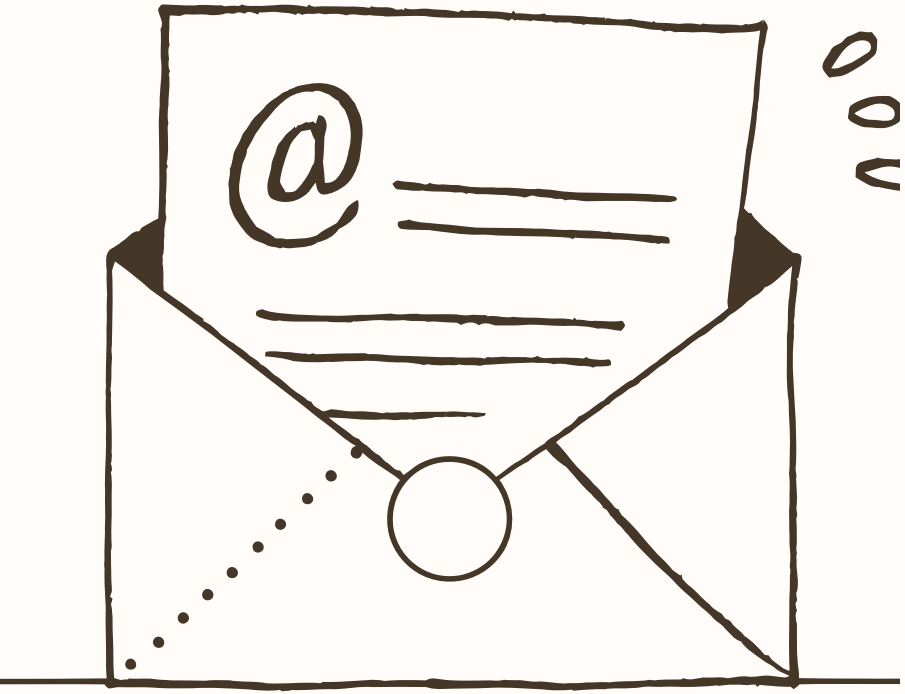


Fałszywe załączniki - jak nie dać się złapać na zainfekowane pliki

Poznasz najczęstsze metody ukrywania złośliwego oprogramowania w plikach oraz praktyczne wskazówki, które pomogą Ci zachować bezpieczeństwo w codziennej pracy z załącznikami.

Czym są fałszywe załączniki?

Ukryte złośliwe oprogramowanie

Pliki zawierające szkodliwy kod, który może aktywować się przy otwarciu, podczas podglądu lub poprzez uruchomienie makr/skryptów.

Pozornie niewinne pliki

Mogą przypominać typowe faktury, plany, CV, oferty, zdjęcia czy formularze - nie muszą wyglądać podejrzanie.

Różne metody aktywacji

Złośliwy kod może uruchomić się automatycznie lub wymagać interakcji użytkownika, np. kliknięcia przycisku "Włącz zawartość".

Co może zrobić zainfekowany plik?

Oprogramowanie szpiegujące

Zainstalować keylogger rejestrujący naciśnięcia klawiszy i przechwytujący poufne dane.

Backdoor

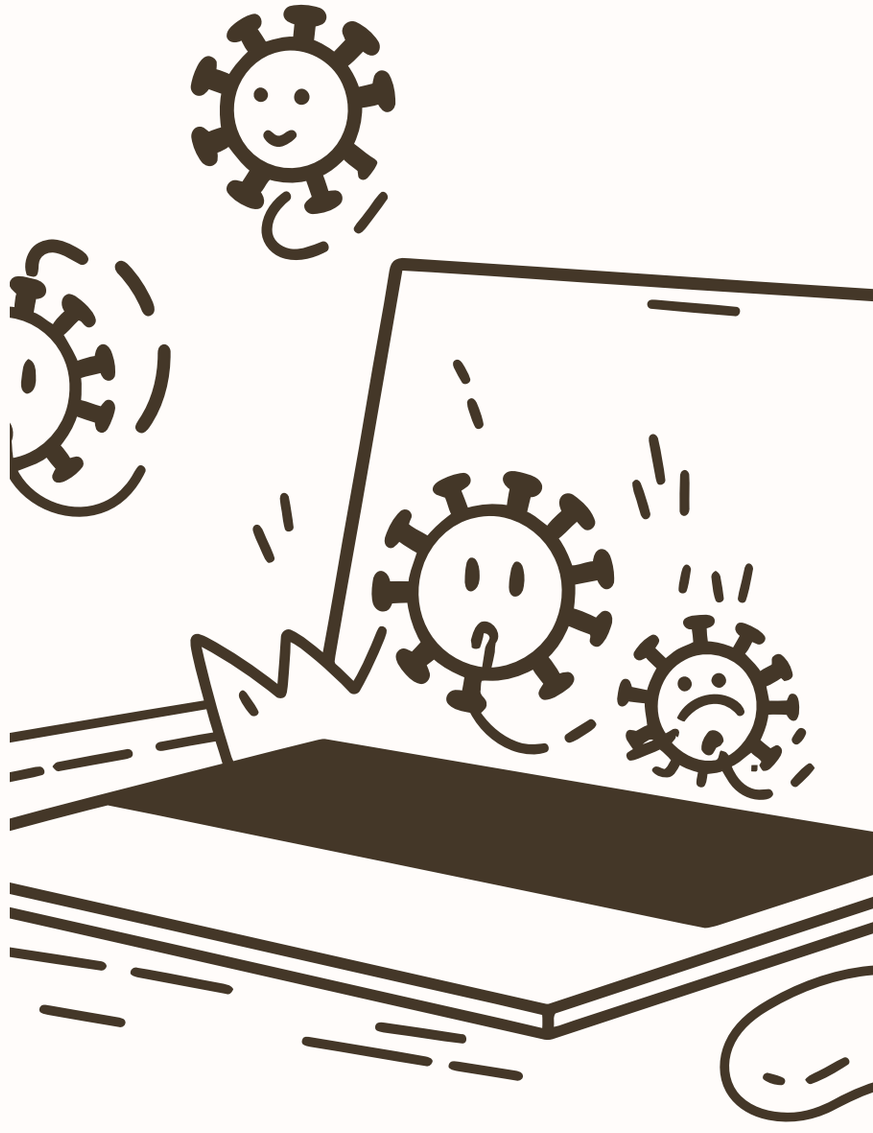
Uruchomić niewidoczny kanał dostępu dla atakującego, umożliwiający kontrolę nad systemem.

Ransomware

Zainicjować szyfrowanie danych i wyłudzenie okupu za ich odblokowanie.

Przejęcie kontroli

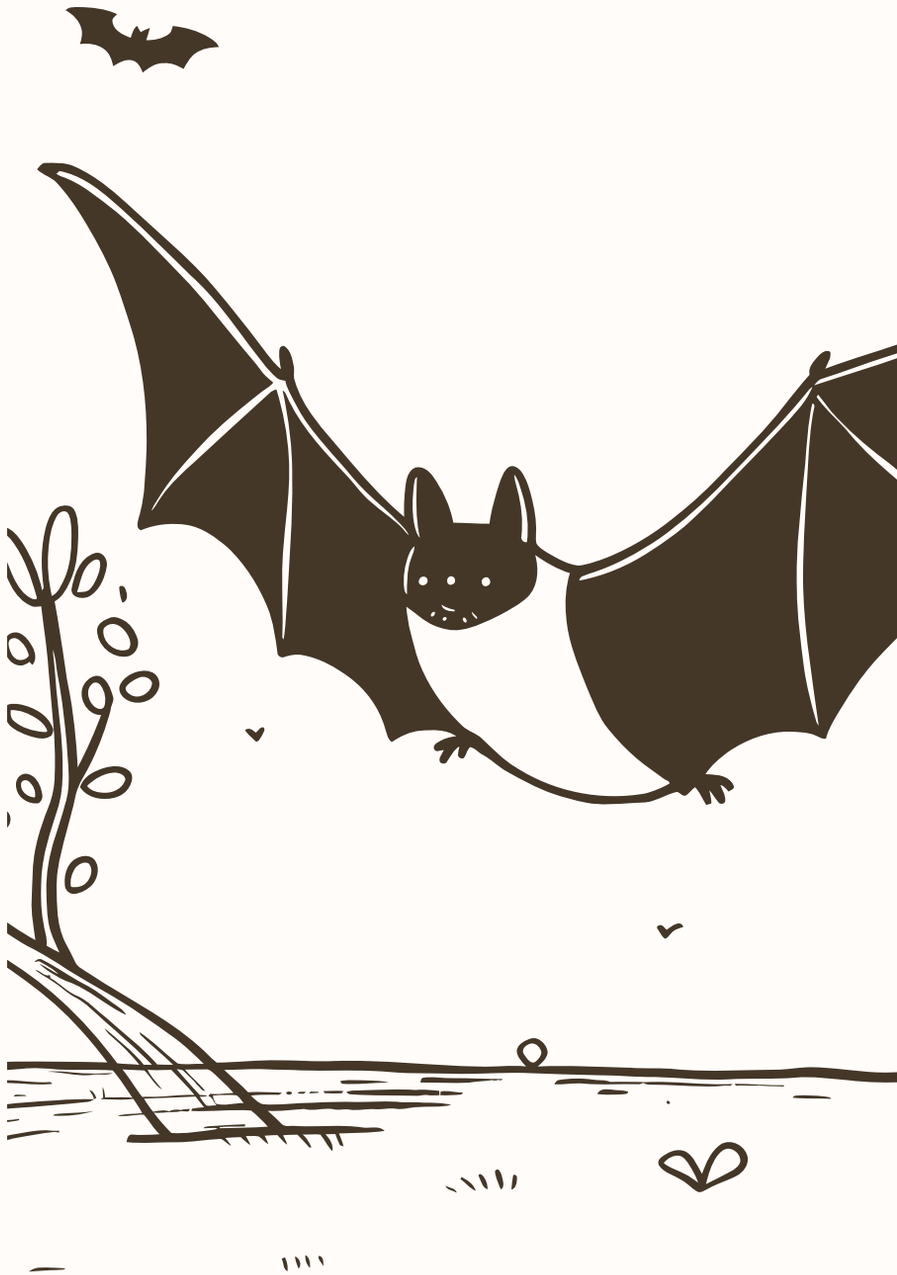
Uzyskać dostęp do plików lokalnych i zasobów sieciowych, przejąć kontrolę nad systemem użytkownika.



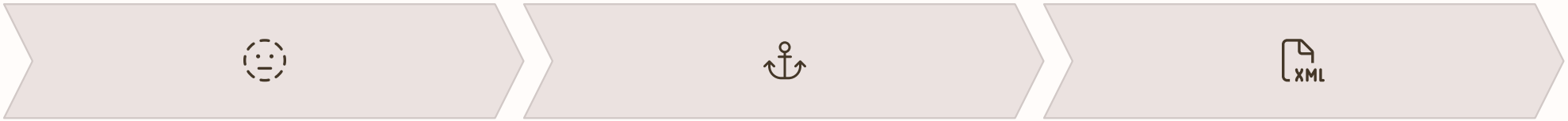
Typowe formaty plików wysokiego ryzyka

Rozszerzenie	Dlaczego może być niebezpieczne?
.exe, .com, .bat, .cmd, .scr	Uruchamiają kod bezpośrednio.
.vbs, .js, .jar	Zawierają skrypty, mogą działać w tle.
.docm, .xlsm, .pptm	Zawierają makra (automatyczne sekwencje czynności).
.txt, .jpg	Zwykle są bezpieczne, ale cyberprzestępcy mogą ukrywać szkodliwe pliki pod nazwami, które tylko udają takie formaty – np. zdjęcie.jpg.exe.

Uwaga: Samo rozszerzenie .pdf lub .docx **nie oznacza bezpieczeństwa**, jeśli plik pochodzi z niepewnego źródła.



Przykłady nietypowych metod infekcji



Ukryte pliki wykonywalne

Plik może nazywać się "Faktura.pdf.exe", a dzięki ustawieniom systemowym rozszerzenie .exe może być niewidoczne.

Pliki osadzone w dokumentach

Excel z osadzonym skryptem VBA, aktywowanym po otwarciu dokumentu.

Podwójne rozszerzenia

"umowa.docx.scr" – pierwsze rozszerzenie myli użytkownika, sugerując bezpieczny dokument.

Wskazówki dla użytkownika

Kwestionuj interakcje

Jeśli plik oczekuje na Twoją interakcję (np. "Włącz zawartość", "Enable Macros"), zastanów się, czy to konieczne.

Zwracaj uwagę na ostrzeżenia

Jeśli system operacyjny wyświetla ostrzeżenie lub pyta o zgodę – nie klikaj odruchowo "Tak".

Używaj firmowych urządzeń

Nie przetwarzaj załączników w urządzeniach prywatnych, które nie mają firmowych zabezpieczeń.

Nie przesyłaj dalej

Nie przesyłaj dalej podejrzanych plików – możesz nieświadomie rozszerzyć skalę zagrożenia.

Dobre praktyki w środowisku pracy

Udostępniaj przez chmurę

Udostępniaj pliki współdzielone przez chmurę zamiast przesyłać je e-mailem jako załącznik.

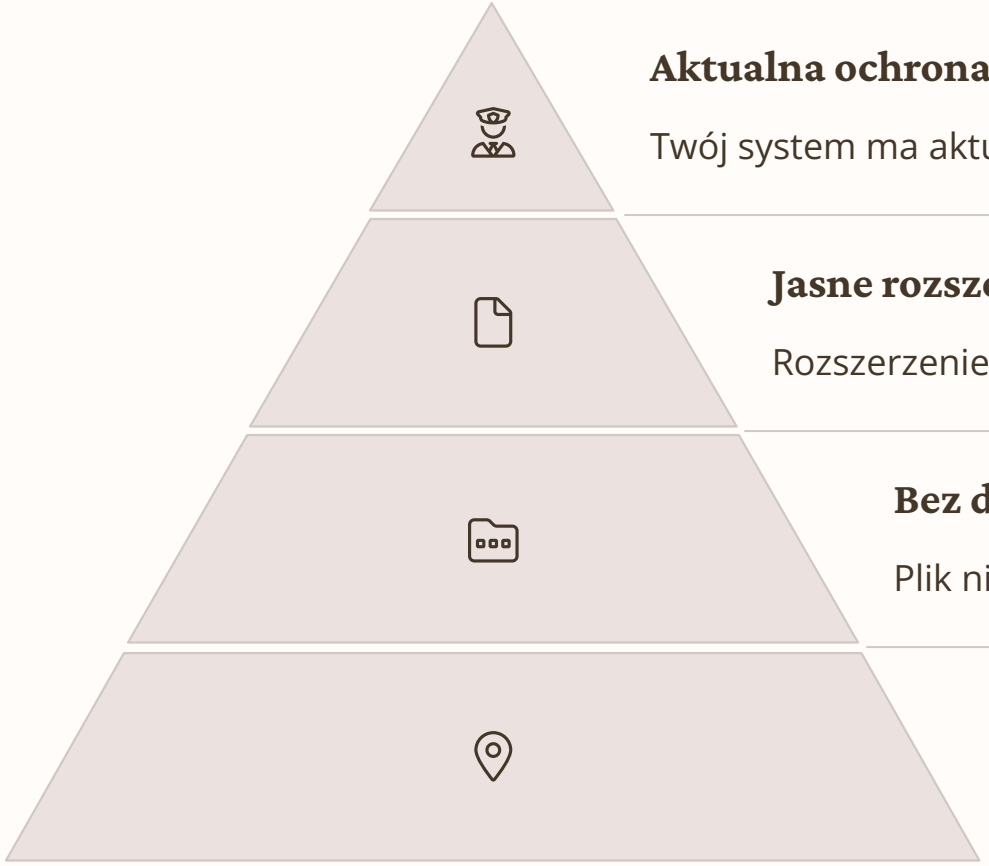
Korzystaj z platform

Korzystaj z centralnych platform udostępniania dokumentów, gdzie dostęp jest kontrolowany.

Szyfruj pliki

Jeśli musisz wysłać plik e-mailem, rozważ jego zaszyfrowanie lub dodanie hasła przekazywanego osobno.

Weryfikacja bezpieczeństwa załącznika – checklista



Aktualna ochrona

Twój system ma aktualny antywirus

Jasne rozszerzenie

Rozszerzenie pliku jest jasne i niebudzące wątpliwości

Bez dodatkowej zawartości

Plik nie wymaga włączenia dodatkowej zawartości lub makr

Znane pochodzenie

Znasz pochodzenie pliku i jest on zgodny z kontekstem

Jeśli odpowiedź na którykolwiek z punktów jest negatywna - NIE otwieraj pliku i skonsultuj się z działem IT!