



Cyberbezpieczeństwo

podstawowe zasady



ZAINSTALUJ SPRAWDZONY PROGRAM ANTYWIRUSOWY

Ważne jest, aby program był regularnie aktualizowany (nie tylko przez Ciebie, ale też przez producenta).



UŻYWAJ BEZPIECZNYCH HASEŁ

Używaj wielkich i małych liter, cyfr, znaków specjalnych itp. Nie zapisuj haseł w dostępnych miejscach, regularnie je zmieniaj oraz nie używaj tego samego hasła do innych kont.



STOSUJ UWIERZYTELNIANIE DWUSKŁADNIKOWE

...czyli dwustopniową weryfikację polegającą na wykorzystaniu do logowania dodatkowego etapu sprawdzania użytkownika.



KORZYSTAJ Z LEGALNEGO OPROGRAMOWANIA

Nie pobieraj oprogramowania, które pochodzi z nieznanych stron lub tych przesłanych drogą e-mailową.



REGULARNIE PRZEPROWADZAJ AKTUALIZACJE

Szczególnie ważne są aktualizacje przeglądarek internetowych oraz poczty.



UŻYWAJ PRZEGLĄDARKI W BEZPIECZNY SPOSÓB

Wyłącz wszystkie niepotrzebne, budzące wątpliwości i nieznane wtyczki. Najlepiej też zrezygnuj z automatycznego zapamiętywania haseł i autouzupełniania formularzy.



NIE PODŁĄCZAJ DO URZĄDZEŃ NIEZNAJANYCH NOŚNIKÓW DANYCH

Mogą zwierać szkodliwe oprogramowanie.



UWAŻAJ NA PUBLICZNE SIECI WI-FI

Szczególnie logując się na konta i przysyłając dane wrażliwe.



RÓB BACKUPY

Twórz kopie zapasowe najważniejszych danych.



BĄDŹ CZUJNY NA DZIAŁANIA HAKERSKIE TYPU PHISHING

Zachowaj ostrożność podczas pobierania plików, klikania w linki i otwierania załączników z wiadomości. Zawsze sprawdzaj nadawcę lub w ogóle zrezygnuj z otwierania e-maili, co do których nie masz pewności.



OPRACUJ PLAN ODTWARZANIA AWARYJNEGO

Z wyprzedzeniem przygotuj procedury działań na wypadek nieplanowanego przestoju spowodowanego atakiem hakerskim.



PAMIĘTAJ O SZKOLENIACH PRACOWNIKÓW

Przeprowadzaj regularne szkolenia pracowników z zakresu cyberbezpieczeństwa oraz przedstawiaj nowym pracownikom firmową politykę bezpieczeństwa sieci IT.



Potrzebujesz wsparcia w zakresie cyberbezpieczeństwa?

Napisz od nas: kontakt@resilia.pl