Jak należy postępować w pracy?

1. Przed wyjściem z pracy **schowaj wszystkie dokumenty** z biurka

2**. Nie zapisuj, nie przyklejaj karteczek z hasłami** na monitorze i na biurku.

3. Wydruki zawierające poufne lub tajne dokumenty **zabieraj od razu z drukarki.**

4. Poufne i tajne dokumenty **niszcz tylko w niszczarce.**

5. **Zmazuj zapisy z tablic po spotkaniach**, od razu po ich zakończeniu.

6. **Nie zostawiaj tokenów z podpisów elektronicznych/ banków** cały czas włożonych do komputera.

7. **Nie zostawiaj urządzeń pendrive, dysków przenośnych** na biurkach lub w komputerze.

8. Wszelkie nośniki pamięci (DVD, pendrive) **przechowuj w szafie zamykanej na klucz.**

9. Poufne dokumenty zamykaj w **szafie zamykanej na klucz** (najlepiej metalowej).

10. **Nie zostawiaj na biurku** kluczy do szafek, pomieszczeń.

11. Jeśli odchodzisz od komputera **zablokuj go- Windows + L.**

12. Jeśli odchodzisz od biurka, **schowaj urządzenia mobilne do szuflady.**

13. Gdy wychodzisz z biura- **wyłącz komputer.**

Ogólne zasady cyberbezpieczeństwa

1. Chroń urządzenia silnymi hasłami.

2. Zainstaluj i aktualizuj system antywirusowy.

3. Włącz ochronę prywatności w przeglądarce oraz kasuj pliki cookies.

4. Uaktualniaj system operacyjny i aplikacje bez zwłoki.

5. Sprawdzaj dostępność połączeń HTTPS.

6. Unikaj korzystania z otwartych sieci Wi-Fi.

7. Korzystaj z komunikatorów obsługujących szyfrowanie (np. Signal)

8. Korzystaj z uwierzytelnienia dwuskładnikowego.

9. Korzystaj z narzędzi czyszczących ślady użytkowania komputera- np. usuwanie danych po przez ich wielokrotne nadpisywanie (uniemożliwienie odtworzenia usuniętych danych).

10. Kontroluj uprawnienia instalowanych aplikacji.

11. Twórz kopie zapasowe.

12. Szyfruj przechowywane wrażliwe dane.

13. Zniszcz fizycznie stare dyski do przechowywania danych.

14. Zachowaj czujność przy otwieraniu e-maili, sms-ów, mms-ów (nie klikaj w podejrzane linki, załączniki).

15. Odwiedzaj tylko zaufane strony internetowe.

16. Sprawdź czy twoje hasło zostało skradzione (po wpisaniu na stronę zmień je)? https://haveibeenpwned.com/

17. Nie podawaj swojego e-maila w Internecie, tam gdzie nie jest to konieczne .

18.Nie podawaj swoich danych osobowych w Internecie, tam gdzie to możliwe.

Poczta e-mail

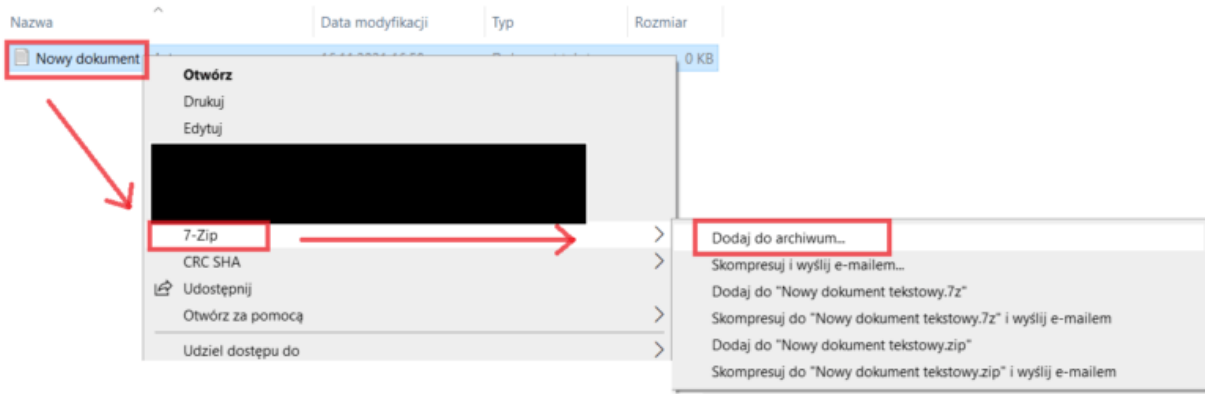
Z poczty mailowej korzystamy codziennie. Służy nam ona zarówno w celach prywatnych, jak i służbowych. Często przesyłamy nią informacje, które nie powinny być dostępne dla osób nieupoważnionych do ich odczytania.

Ochrona informacji przesyłanych za pomocą poczty elektronicznej to bardzo ważna kwestia dotycząca naszego bezpieczeństwa w sieci. Jednym ze sposobów ochrony przesyłanych informacji jest szyfrowanie załączników z wykorzystaniem bezpiecznego szyfrowania symetrycznego. Szyfrowanie poczty elektronicznej minimalizuje ryzyko wycieku poufnych danych i przechwycenie ich przez osoby niepowołane. Istotne jest, iż wszystkie wiadomości e-mail przesyłane w postaci tekstu jawnego, mogą po przechwyceniu zostać łatwo odczytane przez osobę atakującą.

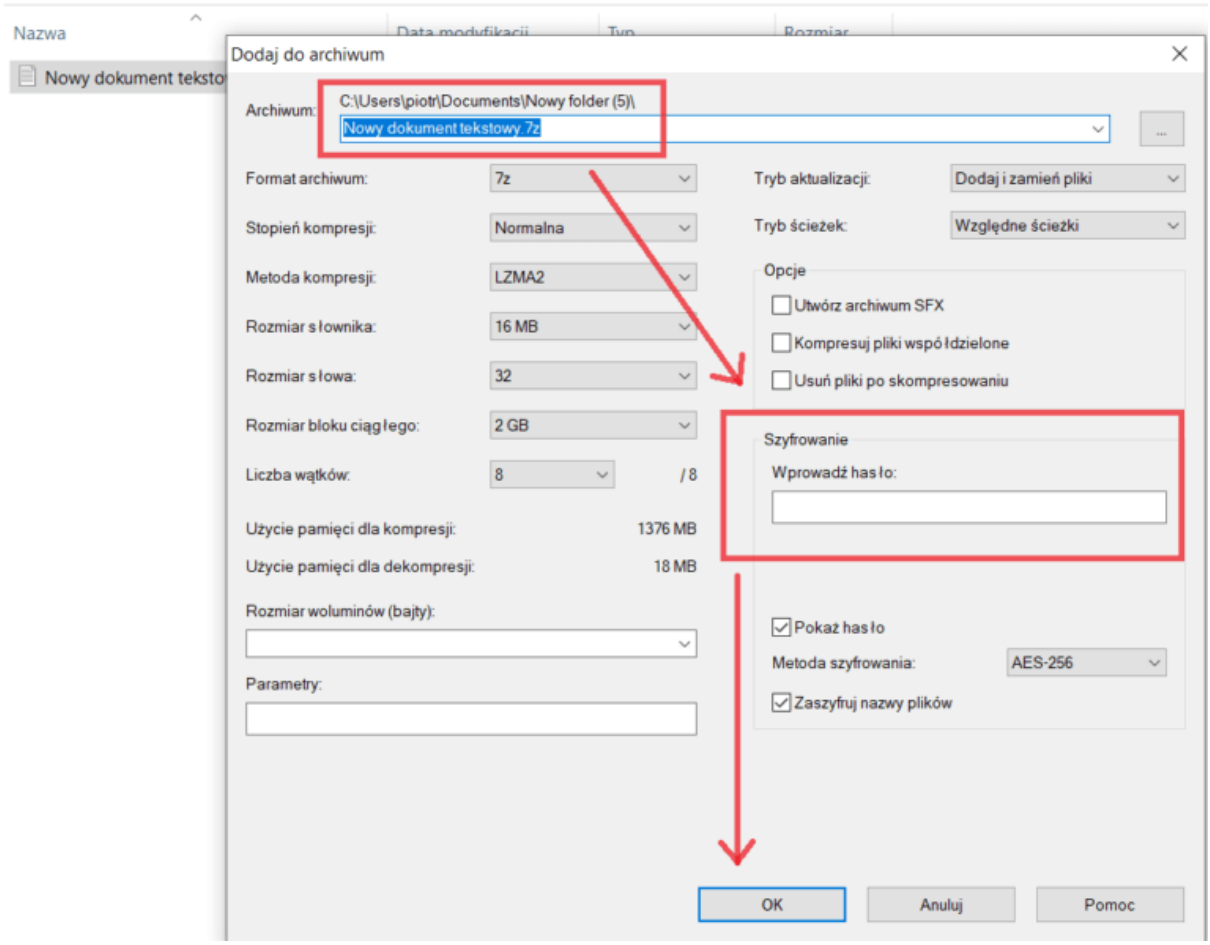
Szyfrowanie załączników poczty to nic trudnego. Przyjrzyjmy się rozwiązaniu szyfrowania załącznika poczty e-mail za pomocą programu do kompresji.
Program 7-zip, umożliwia zaszyfrowanie pliku bezpiecznym algorytmem AES-256.

Szyfrowanie załączników w 4 prostych krokach za pomocą aplikacji 7-zip:

1. Pobierz program 7-ZIP w wersji, która współgra z Twoim systemem operacyjnym ze strony: https://www.7-zip.org/download.html
2. Wybierz plik, który chcesz zaszyfrować i kliknij opcję „Dodaj do archiwum”.



3. Wprowadź nazwę docelowego pliku. Pojawi się wówczas możliwość ustawienia hasła, które zabezpieczy plik przed otwarciem.



Zapamiętaj: Hasło należy przekazać odbiorcy innym kanałem (np. po przez komunikator zapewniający szyfrowanie end-to-end)!

Program umożliwia szyfrowanie jednego lub kilku plików jednocześnie. Należy zaznaczyć, iż pomimo, że wykorzystywany przez program algorytm AES-256 jest aktualnie uznawany za bezpieczny i nie został oficjalnie skompromitowany, jego skuteczność zależy od zapewnienia poufności ustalonego hasła oraz jego „mocy". W przypadku, gdyby ustalone hasło byłoby łatwe do odgadnięcia, atakujący z łatwością odszyfruje chronione informacje.

Tak jak przy korzystaniu z każdego rodzaju oprogramowania, w przypadku programu 7-zip zaleca się śledzić biuletyny bezpieczeństwa, portale branżowe, czy bazy podatności (takie jak CVE), w celu kontroli, czy używana wersja programu nie posiada podatności, które mogłyby zostać wykorzystane przez hackerów.

Należy podkreślić, iż zabezpieczenie pliku hasłem nie zawsze jest równoznaczne z zaszyfrowaniem pliku. Samo zabezpieczenie na poziomie aplikacji nie zapewnia tak wysokiego poziomu bezpieczeństwa informacji, jak wykorzystanie systemów kryptograficznych. W związku z tym, przed wybraniem konkretnego oprogramowania do zabezpieczenia pliku, należy zweryfikować, czy posiada on funkcjonalność zaszyfrowania danej informacji.

Jak budować hasła?

Pamiętaj, aby wykorzystywać silne hasło. Należy używać haseł, które:

a) składają się z minimum 12 znaków i pięciu słów,
b) są trudne do odgadnięcia,
c) nie są logiczne i powiązane z twoim otoczeniem (zaleca się łączyć wyrazy polskie ze słowami z języka obcego lub tworzyć w haśle opis abstrakcyjnych sytuacji)
d) nie zawierają sekwencji znaków na klawiaturze, typu „Qwerty12”, „1QAZ@wsx” itp.),
e) nie są popularnym, znanym hasłem (przykład: password, admin itd.)
f) nie są związane z użytkownikiem lub jego rodziną tzn. nie zawierają np.:
- identyfikatora użytkownika (loginu),
- inicjałów,
- nazwisk,
- imion,
- pseudonimów
- dat osobistych np. urodzenia,
- miesięcy (np. Czerwiec#2021, Lipiec#2021),
- numerów telefonu,
- numerów rejestracyjnych samochodów.

Najpopularniejsze zagrożenia cybernetyczne

1. Złośliwe oprogramowania (malware)
2. Ataki z wykorzystaniem złośliwego kodu na stronach internetowych
3. Phishing, czyli bezpośrednie wyłudzanie poufnych informacji lub za pomocą złośliwego oprogramowania
4. Ataki na aplikacje internetowe
5. SPAM – niechciana korespondencja
6. Ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu
7. Kradzież tożsamości
8. Naruszenie poufności, integralności lub dostępności danych
9. Zagrożenia wewnętrzne powodowane przez pracowników
10. Botnet-y – sieci komputerów przejętych przez przestępców
11. Ingerencja fizyczna, uszkodzenia oraz kradzież
12. Wyciek danych
13. Ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych
14. Cyberszpiegostwo
15. Kradzież kryptowalut (cryptojacking)