# Temat główny: Przestępstwa przeciw ochronie informacji

## Ćwiczenie

| | |
|---|---|
| **Cel główny** | Ćwiczenie pozwoli poznać/utrwalić nawyki/metody dotyczące stosowania dwuskładnikowego uwierzytelniania (2FA - two-factor authentication). |
| **Czas trwania** | Około 40 minut |
| **Cel aktywności** | Dowiedzieć się, jaka jest wiedza uczestników odnośnie stosowania dwuskładnikowego uwierzytelniania, wskazać, jakie są korzyści ze stosowania tych zabezpieczeń, pokazać jak włączyć/ uruchomić dwuskładnikowe uwierzytelnianie na przykładzie Allegro/ Facebook/ poczta internetowa/ ePUAP |
| **Potrzebne materiały** | Telefon/tablet/komputer z dostępem do Internetu, tablica, pisaki, kartki |
| **Instrukcje** | – Poproś uczestników o napisanie na kartkach przykładów uwierzytelniania dwuskładnikowego (dwuetapowa weryfikacja), jeśli znają to pojęcie, lub z czym im się ono kojarzy np.: kody jednorazowe lub linki wysyłane przez e-mail, kody jednorazowe wysyłane przez SMS, kody czasowe w aplikacji, klucz sprzętowy (do 5 min)<br>– Udziel wskazówek odnośnie możliwości włączenia dwuetapowej weryfikacji dostępu do różnych kont<br>– Poproś uczestników o wypisanie na tablicy swoich przykładów z kartek oraz na wskazanie miejsc, gdzie warto korzystać z tego rodzaju zabezpieczeń (np.: strona banku, serwisu aukcyjnego, konto email, serwis społecznościowy)<br>– Przeprowadź dyskusję w grupie na temat stosowania dwuetapowego uwierzytelniania oraz plusów i minusów stosowania konkretnych metod zabezpieczeń, może być w formie wspólnego uzupełnienia tabeli (do 15 minut). |

Erasmus+
Współfinansowany w ramach programu Unii Europejskiej Erasmus
is better life

## Przykładowa tabela do ćwiczenia

| Metoda drugiego etapu weryfikacji | Plusy/ zalety | Minusy/ wady |
|---|---|---|
| kody jednorazowe lub linki wysyłane przez e-mail | | |
| kody jednorazowe wysyłane przez SMS | | |
| kody czasowe w aplikacji | | |
| klucz sprzętowy U2F | | |
| biometria - twarz, głos, odcisk palca | | |
| | | |

Zwroty do wykorzystania:

- można przechwycić, przekierować
- trzeba udostępnić swój nr telefonu
- dodatkowy koszt
- łatwość obsługi/ konfiguracji
- odporny na ataki typu phishing
- podatny na ataki typu phishing
- konieczność bycia online
- urządzenie musi być naładowane/ dostępne

Erasmus+
Współfinansowany
w ramach programu
Unii Europejskiej Erasmus
is better life