Biznes i zarządzanie

www.biznesizarzadzanie.pl

SCENARIUSZ LEKCJI

Cyberbezpieczeństwo

Materiał jest częścią projektu Bankowcy dla Edukacji Finansowej Dzieci i Młodzieży BAKCYL i Projektu Bezpieczeństwo w Cyberprzestrzeni
www.bakcyl.wib.org.pl
www.cyber.wib.edu.pl

BAKCYL
Bankowcy dla Edukacji Finansowej Dzieci i Młodzieży

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

Materiał przygotowany przez Fundację Warszawski Instytut Bankowości w ramach projektu wspierającego wdrażanie przedmiotu biznes i zarządzanie z wykorzystaniem materiałów projektu Porwani przez Ekonomię
www.PorwaniPrzezEkonomie.pl

Po przebytej lekcji uczeń:

- ma świadomość zagrożeń występujących w cyberprzestrzeni,
- rozumie, że nie warto dzielić się niektórymi informacjami w sieci i wie dlaczego tak jest,
- potrafi zadbać o swoje bezpieczeństwo w sieci,
- określa dlaczego bezpieczne hasło to podstawa funkcjonowania w Internecie,
- tworzy bezpieczne hasła, aby były silne i jednocześnie łatwe do zapamiętania,
- identyfikuje metody socjotechniczne (m.in. phishing),
- wie jak korzystać z ustawień prywatności w social mediach,
- potrafi bezpiecznie korzystać ze smartphone'a,
- potrafi bezpiecznie korzystać z bankowości elektronicznej.

W niniejszym scenariuszu:

- definicje, które należy wprowadzić są podkreślone,
- *informacje, które prowadzący powinien powiedzieć uczniom (swoimi słowami) są zapisane kursywą.*

Slajd 1. Bankowcy dla Edukacji Finansowej Dzieci i Młodzieży BAKCYL

INFORMACJA DLA NAUCZYCIELA:

Celem projektu edukacyjnego Bankowcy dla Edukacji Finansowej Dzieci i Młodzieży BAKCYL jest podnoszenie poziomu wiedzy z zakresu ekonomii, cyberbezpieczeństwa oraz inspirowanie świadomych działań i budowanie właściwych postaw w zakresie przedsiębiorczości. Projekt jest częścią jednego z największych programów pozaformalnej edukacji finansowej w Europie – **„Bankowcy dla Edukacji"**

Przejdź do tematu lekcji:

Slajd 2. Wprowadzenie do lekcji.

➢ *Na dzisiejszej lekcji będziemy rozmawiać o cyberbezpieczeństwie. Temat jest ważny, choćby z tego powodu, że do cyberprzestrzeni przeniosło się wiele naszych codziennych aktywności – rozrywka, zakupy, praca czy nauka. Zagrożeń w sieci jest coraz więcej – w trakcie pandemii skala i liczba cyberataków jeszcze się zwiększyła. Pokażemy dziś kilka przykładów zagrożeń, na które wszyscy jesteśmy narażeni, zwrócimy również uwagę na najważniejsze kwestie w zakresie cyberbezpieczeństwa w kilku głównych obszarach tematycznych.*

- *Zwrócimy uwagę przede wszystkim na to, na co sami mamy wpływ czyli bezpieczeństwo od strony „przeciętnego" użytkownika. Zasady, o których porozmawiamy możemy nazwać tzw. „higieną w sieci".*

Slajd 3. Ofiarą cyberataku może być każdy z nas. Codziennie.

- *Warto zdać sobie sprawę z tego, że codziennie każdy z Was może stać się ofiarą cyberataku. Może to się stać w sposób bezpośredni np. przez Waszą pocztę elektroniczną lub media społecznościowe ale także w sposób „pośredni" np. zostaną zaatakowane serwery urzędu, szkoły, firmy, na których są Wasze dane i w ten sposób wpadną one w ręce cyberprzestępców.*
- *Skupimy się dziś na tym co sami możemy zrobić, żeby uniknąć cyberataków.*

Slajd 4. Który adres wybierzesz?

- *Żeby uświadomić Wam, że zagrożenie dotyczy każdego z nas przeprowadźmy małe ćwiczenie. Załóżmy, że jesteście wszyscy klientami banku, który nazywa się „Monika Bank" i ma stronę internetową www.monikabank.pl. Chcecie wejść na stronę banku, zalogować się do bankowości internetowej – sprawdzić stan konta, zrobić przelew itd.*
- *Który z podanych adresów internetowych uznacie za prawidłowy (bezpieczny) do zalogowania się do Waszej bankowości?*

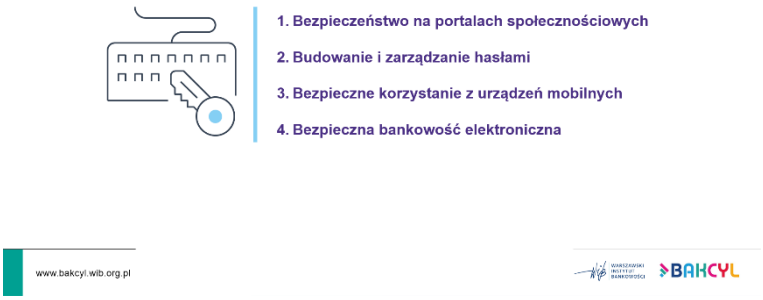
https://monikabank.logowanie.pl/
www.logowanie.monikabank.pl/

Większość uczniów zazwyczaj wybiera link nr 1., który jest błędny. Prawidłowy jest link nr 2. Warto zwrócić uwagę na to, że pierwszy nie prowadzi do witryny monikabank.pl tylko do witryny logowanie.pl. Przy weryfikacji poprawności adresów internetowych warto zwracać uwagę na to, co znajduje się bezpośrednio przed rozszerzeniem czyli .pl, .com itd. „Zielona kłódka", protokół „https" (certyfikat SSL) przed adresem strony nie daje nam gwarancji, że trafiamy pod właściwy adres. Mamy wtedy informację, że połączenie ze stroną jest szyfrowane, ale w dalszym ciągu może być to strona założona przez cyberprzestępców. Certyfikat SSL można wykupić za kilkadziesiąt złotych.

Podkreśl, że chcąc skorzystać z bankowości elektronicznej, adres strony www banku należy wpisać samodzielnie. Nie powinno się korzystać z wyszukiwarek (np. google), które mogą nas zaproponować kilka adresów www banku, w tym fałszywe.

Dodatkowe informacje:

Jeśli „Monika Bank” faktycznie by istniał i miał stronę o podanym adresie to wpisanie go w przeglądarkę spowodowałoby automatyczne przekierowanie na protokół https czyli pełen adres wyglądałby następująco https://www.logowanie.monikabank.pl/



Slajd 5. Wskazanie obszarów tematycznych, które będą poruszone na lekcji.

- *Będziemy omawiać tematykę cyberbezpieczeństwa w czterech obszarach tematycznych – portale społecznościowe, hasła, urządzenia mobilne oraz bankowość elektroniczna.*
- *Wspólnym mianownikiem dla tych czterech obszarów jest bezpieczeństwo naszych danych osobowych – to one często są głównym celem cyberprzestępców.*

Slajd 6. Portale społecznościowe

- Przechodzimy do pierwszego obszaru tematycznego – Portale społecznościowe.
- *Portale społecznościowe stają się coraz popularniejsze – na całym świecie korzysta z nich ponad 4 mld użytkowników *, w Polsce prawie 26 mln osób*Największym zagrożeniem w social mediach jest lekkomyślność użytkowników, którzy często sami udostępniają zbyt wiele informacji na swój temat.*
- Zapytaj uczniów z jakich portali społecznościowych korzystają.

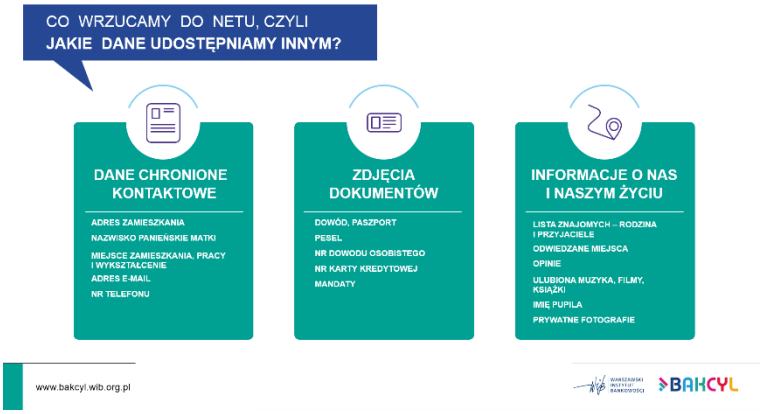
* www.mobirank.pl/2020/10/20/digital-10-2020-juz-ponad-4-mld-uzytkownikow-social-mediow/

* www.empemedia.pl/social-media-w-polsce-2021-nowy-raport/

Slajd 7. Cytat – Stanisław Lem.

Stanisław Lem (znany pisarz s-f, futurolog) powiedział kiedyś, że żyjemy w świecie, w którym jest za mało rozumu, a za dużo informacji. Ten cytat wydaje się jeszcze bardziej aktualny dzisiaj. W internecie mamy dostęp do miliardów informacji, które trudno objąć rozumem. Być może właśnie dlatego niektórym użytkownikom tego

rozumu brakuje 😊. Często to właśnie sami użytkownicy lekkomyślnie umieszczają w internecie zbyt wiele informacji na swój temat.



Slajd 8. Jakie dane udostępniamy innym w internecie.

- *Dane, które umieszczamy w sieci mogą zostać wykorzystane do przeprowadzania rożnego rodzaju wyłudzeń lub do śledzenia. Absolutnie nie powinniśmy umieszczać w internecie zdjęć dokumentów tożsamości lub publikować swoich danych osobowych.*
- *Rozsądnie podchodźmy również do publikowani informacji np. na temat swoich zainteresowań. Zwróćmy uwagę np. na to, że nazwisko panieńskie (swoje lub mamy) jest często jednym z pytań weryfikacyjnych na różnego rodzaju infoliniach.*

Zaprezentuj film: Nie publikuj danych!

https://www.youtube.com/watch?v=bB82IGAllNE&list=PLvWZa2ao-01CrzDwv8yD2jWYUUADsbTj5&index=6

Po projekcji wróć do prezentacji.

Slajd 9. Kto jest właścicielem Twoich danych?

- *Dane, które umieszczamy w internecie powinniśmy traktować jako publiczne. Ustawienia prywatności mogą pomóc w zapewnieniu, że Twoje posty są widoczne tylko dla wybranego grona osób, ale ustawienia z nimi związane często się zmieniają i bywają niejednoznaczne. To co kiedyś było prywatne, może nagle stać się publiczne. Pamiętaj też, że prywatność Twoich wpisów jest zależna od tego z kim się nimi dzielisz. Im więcej osób może przeczytać Twój post, tym bardziej prawdopodobne, że stanie się on publiczny. Najlepiej będzie, jeśli założysz, że cokolwiek co umieszczasz w sieci, prędzej czy później stanie się publicznie dostępne i niemożliwe do usunięcia. Odpowiadając na pytanie: Kto jest właścicielem Twoich danych (np. umieszczonych na Facebooku) – właścicielem pozostajesz Ty, ale warto zapoznać się z regulaminem Facebooka, aby zobaczyć komu i jakiej licencji udzielamy.*

DODATKOWE INFORMACJE DLA NAUCZYCIELA:

Fragment regulaminu Facebooka (na dzień 29.08.2021 r.):

„Szczególnie w przypadku udostępniania, publikacji lub przesyłania treści objętych prawami własności intelektualnej w naszych Produktach lub w powiązaniu z nimi użytkownik udziela nam licencji niewyłącznej, zbywalnej, obejmującej prawo do udzielania sublicencji, bezpłatnej i globalnej do

korzystania, wykorzystywania, dystrybuowania, modyfikowania, uruchamiania, kopiowania, publicznego odtwarzania lub wyświetlania, tłumaczenia jego treści i tworzenia na ich podstawie utworów pochodnych (zgodnie z wybranymi przez użytkownika ustawieniami prywatności i aplikacji). Oznacza to na przykład, że udostępniając zdjęcie na Facebooku, użytkownik udziela nam zgody na przechowywanie, kopiowanie i udostępnianie go innym użytkownikom (w tym przypadku też zgodnie z ustawieniami swojego konta), np. dostawcom usług obsługującym nasz serwis lub inne produkty Facebooka, z których użytkownik korzysta. Licencja wygaśnie w momencie usunięcia treści użytkownika z naszych systemów".

Slajd 10. Co atakujący może zrobić z moimi danymi?

➢ *Przestępcy mogą wykorzystać dane, żeby się pod nas podszywać w sieci i np. kontaktować się z naszymi znajomymi wykorzystując komunikatory i media społecznościowe. Jeśli zdobędą dostęp do naszych danych osobowych i zdjęć dokumentów, to mogą je wykorzystać do przeprowadzenia prób wyłudzeń finansowych – zaciągnięcia kredytu, pożyczki na Twoje dane lub zakupów on-line.*

Slajd 11. Zastrzegaj utracone dokumenty w banku!

➢ *Dbaj o swoją tożsamość. W przypadku zagubienia lub kradzieży dokumentu tożsamości (m.in. dowodu osobistego, paszportu, prawa jazdy) zgłoś ten fakt w banku. Nie wystarczy zgłoszenia na Policji lub w Urzędzie Miasta/Gminy. Zgłoszenie w banku oznacza wpisania dokumentu do bazy Dokumentów Zastrzeżonych, z której korzystają wszystkie banki. W przypadku posłużenia się Twoim zastrzeżonym dokumentem przez inną osobę, taka próba zostanie zablokowana.*

Slajd 12. 828 828 828

➢ *Jeśli masz podejrzenie, że dane twojej karty mogły zostać skradzione (lub zgubiłeś/ukradziono Ci kartę) lub z jakiś powodów sam wrzuciłeś jej zdjęcie do netu to zastrzeż ją korzystając z numeru* ***828 828 828.***

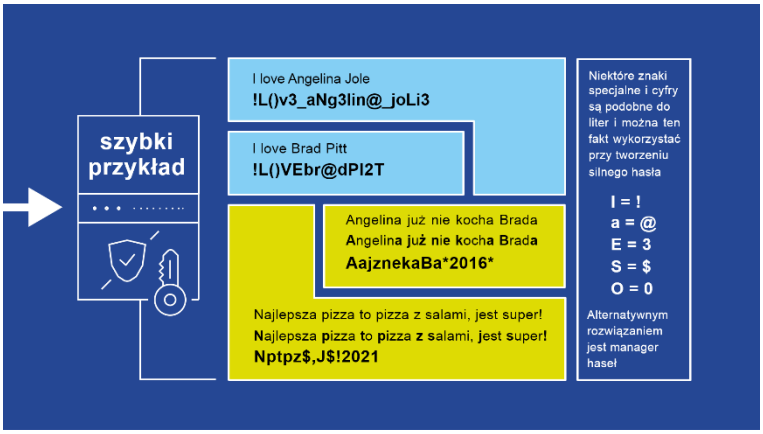
Slajd 13. Budowanie i zarządzanie hasłami

➢ Przechodzimy do drugiego obszaru tematycznego – Budowanie i zarządzanie hasłami.

➢ *Słabe hasło jest jednym z najczęstszych powodów utraty naszych danych, dlatego przechodzimy do kolejnego bardzo ważnego obszaru jakim są hasła.*

Slajd 14. Jak stworzyć bezpieczne hasło.

➢ *Bezpieczne hasło to przede wszystkim hasło długie - 12 znaków to minimum. Zastosuj w nim również kombinację małych i dużych liter, cyfr i znaków specjalnych.*



Slajd 15. Przykłady mocnych haseł.

➢ *Widzimy kilka przykładów haseł stworzonych na podstawie łatwych do zapamiętania zdań. Warto wykorzystywać ten schemat przy tworzeniu swojego bezpiecznego hasła. W tym przykładzie wykorzystujemy pierwszą literę z każdego wyrazu w danym zdaniu. Część liter zapisujemy jako duże. Warto wykorzystać to, że niektóre litery są podobne do znaków specjalnych lub cyfr. W ten sposób stworzymy silne hasło, które będzie jednocześnie łatwe do zapamiętania. Alternatywnym rozwiązaniem jest korzystanie z managera haseł.*

DODATKOWE INFORMACJE DLA NAUCZYCIELA:

Podane przykłady są jedynie inspiracją w jaki sposób można zapamiętywać trudne i długie hasła. Poniżej informacja jakiego schematu użyto do zapamiętania hasła:

„I love Brad Pitt" – drugi i czwarty wyraz pisany w całości dużymi literami, trzeci wyraz w pisany małymi literami, a dodatkowo poszczególne litery zostały zamienione na znaki specjalne, np. o to (), tt to 2T w

wyniku czego otrzymaliśmy „!L()VEbr@dPI2T”. Warto zachęcić uczniów aby każdy indywidualnie znalazł swój sposób na „szyfrowanie” haseł.

Slajd 16. Bezpieczne korzystanie z urządzeń mobilnych.

- Przechodzimy do trzeciego obszaru tematycznego – Bezpieczne korzystanie z urządzeń mobilnych.
- *Najczęściej do łączenia się z internetem wykorzystujemy urządzenia mobilne, przede wszystkim smartfony, dlatego omówimy teraz najważniejsze zasady bezpiecznego korzystania z tych urządzeń.*
- *Smartfon jest również coraz częściej wykorzystywanym narzędziem do korzystania z bankowości elektronicznej.*

Slajd 17. Smartfon i tablet to komputer.

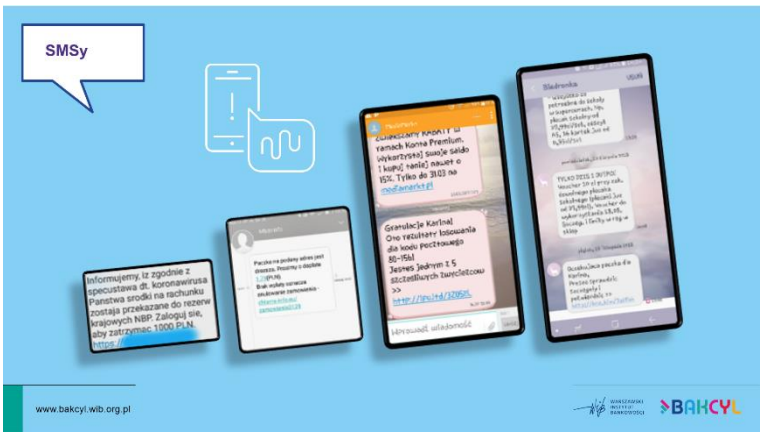
- *Przede wszystkim traktujmy swoje urządzenie mobilne jak komputer osobisty. Wykorzystujemy je przecież do poczty elektronicznej, mediów społecznościowych lub bankowości mobilnej. Dlatego powinniśmy to urządzenie zabezpieczyć tak, jak swój komputer*

Slajd 18. Jak bezpiecznie korzystać z urządzeń mobilnych.

- Omów zasady bezpieczeństwa na urządzeniu mobilnym:
- *Podstawowym zabezpieczeniem Twojego smartfona jest blokada ekranu – zadbaj o to, żeby była silna – blokada biometryczna powiązana z kodem to najbezpieczniejsze rozwiązanie*
- *Zainstaluj oprogramowanie antywirusowe**
- *Zwracaj uwagę czy aplikacja, którą instalujesz nie prosi Cię o nadmierny dostęp do Twoich danych – np. aplikacja latarki nie potrzebuje dostępu do lokalizacji, sms-ów czy kontaktów*

- *Korzystaj tylko z oficjalnych sklepów na Twoją platformę mobilną i zwracaj uwagę na popularność i opinie aplikacji, którą instalujesz*
- *Wyłącz moduł wifi i bluetooth, gdy z niego nie korzystasz. Smartfon z włączonymi modułami może połączyć się z niezabezpieczoną otwartą siecią wifi np. w miejscu publicznym.*
- *Pamiętaj o aktualizacji aplikacji i systemu – możesz włączyć funkcję automatycznych aktualizacji*
- *Nie oddawaj telefonu innej osobie bez usunięcia np. smsów, plików tymczasowych, czy historii przeglądarki stron internetowych.*

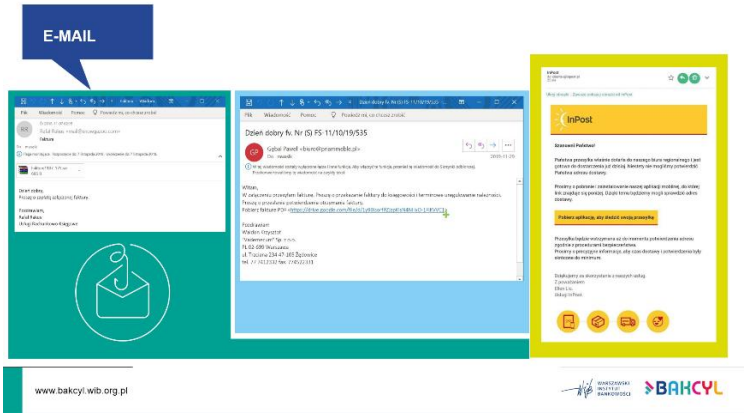
*Dotyczy urządzeń z Android lub Windows Mobile. Platforma iOs (Apple) nie umożliwia zainstalowanie „klasycznego" antywirusa a jedynie aplikacje zwiększające bezpieczeństwo.



Slajd 19. Przykłady prób wyłudzeń.

➢ *Przestępcy bardzo często wykorzystują sms-y do tzw. kampanii phishingowych. To bardzo popularna metoda, która polega na podszywaniu się pod znane firmy, urzędy itd. i wysyłaniu informacji zawierających zainfekowane pliki lub linki prowadzące do stron wyłudzających dane. Nie ufaj takim wiadomościom i nie klikaj w linki, które się w nich znajdują!*

Slajd 20. Przykłady prób wyłudzeń.



➢ *Z phishingiem spotkasz się również korzystając z maila. Uważaj na wiadomości, w których ktoś podszywa się pod znaną Ci firmę czy urząd i wysyła np. fakturę do pobrania.*

➢ *Zweryfikuj dokładnie adres nadawcy, treść i dane zawarte w mailu. Jeśli masz jakiekolwiek wątpliwości nie klikaj w linki, nie pobieraj załączników – usuń podejrzaną wiadomość.*

Slajd 21. Bezpieczna bankowość elektroniczna

➢ *Przechodzimy do czwartego (ostatniego) obszaru tematycznego – Bezpieczna bankowość elektroniczna.*

Slajd 22. Z usług banku możesz korzystać na wiele sposobów.

- *Z bankowości elektronicznej możemy skorzystać na 3 sposoby – poprzez bankowość internetową czyli stronę www banku, aplikację mobilną zainstalowaną na smartfonie czy tablecie oraz poprzez kartę płatniczą.*
- *W każdym z tych obszarów możemy spotkać się z różnymi rodzajami cyberzagrożeń.*

Slajd 23. Jak bezpiecznie korzystać z bankowości elektronicznej.

- Wymień zasady wskazane na slajdzie.

Sajd 24. Bankowe Centrum Cyberbezpieczeństwa.

- *Nad bezpieczeństwem klientów bankowości czuwa m.in. Bankowe Centrum Cyberbezpieczeństwa, które współpracuje z Narodowym Centrum Cyberbezpieczeństwa.*
- Podkreśl, że sektor bankowy jest liderem cyberbezpieczeństwa i możemy się czuć bezpiecznie korzystając z bankowości elektronicznej. Musimy jednak pamiętać, aby dbać o bezpieczeństwo naszych urządzeń i ciągle podnosić wiedze o cyberbezpieczeństwie. Bardzo dużo zależy od wiedzy i postaw klientów banków.

Więcej informacji na: www.wib.org.pl/polacy-w-cyberprzestrzeni-aktywni-zadowoleni-ale-czy-wystarczajaco-rozsadni/

Slajd 25. Co zrobić jeśli padniemy ofiarą cyberataku?

➢ *Podejmij odpowiednie kroki jeśli podejrzewasz, że padłeś ofiarą cyberataku.*

Slajd 26. Podsumowanie.

➢ Przypomnij najważniejszych zasady bezpieczeństwa omówione podczas dzisiejszej lekcji.

Slajd 27. Zakończ lekcję.

➢ Zapytaj czy są pytania,

➢ Podziękuj uczniom.