



OSINT / Social engineering

Wydział Informatyki i Telekomunikacji

Katedra Telekomunikacji i Teleinformatyki

Zaawansowane testy penetracyjne

Prowadzący: Dr inż. Michał Walkowski

Rok akademicki 2022/2023

Autor:

Tomasz Nadrowski



OSINT



Podstawowe informacje o ofierze

- Data urodzenia: 27.08.1999
- Pochodzenie: Giżycko
- Aktualne miejsce zamieszkania: Wrocław
- Edukacja:
 - szkoła podstawowa nr 3 w Giżycku – prawdopodobnie
 - gimnazjum nr 3 w Giżycku
 - I LO w Giżycku
 - Politechnika Wrocławska:
 - 1 st. – inżynier, spec. Bezpieczeństwo danych
 - 2 st. – magister
- E-mail prywatny
- E-mail służbowy – według schematu firmowego
- Nr telefonu
- Praca
- Rodzina – wujek
- Zainteresowania:
 - pływanie
 - koszykówka



Data urodzenia



PŁYWANIE

**Drużynowe Mistrzostwa Warmii i Mazur Szs Olsztyn 2014 –
Szkolny medal to pamiątka na całe życie**

11 grudnia 2014, 16:33

gimnazja

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]
7. [REDACTED] **99 Gim 3 Gzycko 42.58 309**



Pochodzenie

Informacje

Przegląd

Praca i wykształcenie

Wcześniejsze miejsca zamieszkania

Dane kontaktowe i podstawowe informacje

Brak miejsc pracy do wyświetlenia

Brak szkół do wyświetlenia

Z: Giżycko

Brak informacji o związku do wyświetlenia

← [REDACTED] :

[REDACTED]

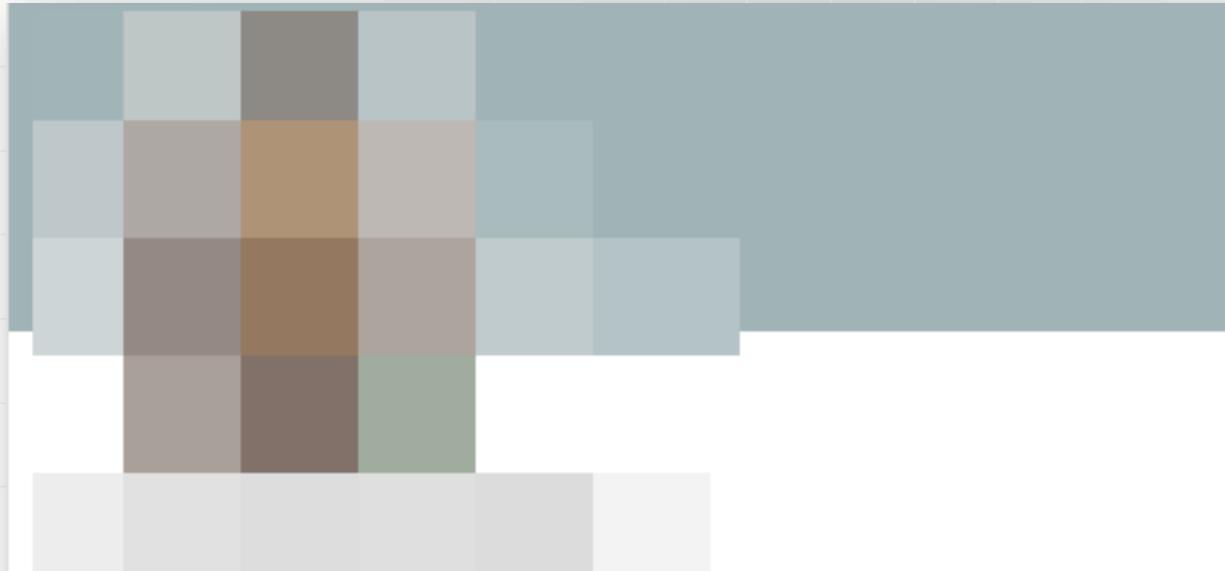
33 Posty 102 Obserwujący 157 Obserwuje

Giżycko
Obserwuję to [REDACTED]

Wysłano prośbę



Aktualne miejsce zamieszkania



Software Tester

Wrocław, Woj. Dolnośląskie, Polska · [Informacje kontaktowe](#)



Edukacja – szkoła podstawowa

23 czerwca 2015 · ...

Szkoła Podstawowa nr 3 w Giżycku – zdedybowany(a).

22 czerwca 2015 ·

Drodzy uczniowie i rodzice ...
Tradycyjnie część z Was na zakończenie roku szkolnego wybiera się do szkoły z kwiatem lub czekoladą w podzięce za rok zmagani.
Rada Pedagogiczna zwraca się z prośbą, aby zamiast tego wpłacić drobną sumę na rzecz Krystiana Czyrko!
Nauczyciele proszą, aby zamiast kwiatów wrzucać pieniązki do puszek w klasopracowniach ...
Prosimy o przychylenie się do inicjatywy i nie kupowanie kwiatów! !!
"Kupimy szansę na zdrowie Krystianowi!"
Wrzucamy po kilka złotych dla naszego ucznia!
Puszki będą czekały w pracowniach w piątek!!!!!!
Prosimy o lajki i promocję inicjatywy wśród naszej społeczności



Edukacja – gimnazjum

gimnazja

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]
7. [REDACTED] 99 Gim 3 Gzycko **42.58** 309



Edukacja – liceum

**Mistrzostwa Województwa w drużynowych zawodach w pływaniu dziewcząt
Licealiada Dziewczęta Rocznik 1998 i młodsí II miejsce**

**Rocznik 1998 i młodsi Dziewczęta 50m klasyczny
3e II miejsce**



Edukacja – uczelnia wyższa

Wykształcenie



Politechnika Wrocławska

Magister inżynier (Mgr inż.), Cyberbezpieczeństwo

2022 – 2023



Politechnika Wrocławska

Inżynier (Inż.), Cyberbezpieczeństwo

2018 – 2022

Specjalizacja: Bezpieczeństwo danych



E-mail prywatny

Zweryfikowane konto

Numer telefonu powiązany z tym kontem został zweryfikowany.
Więcej informacji o [weryfikacji konta](#).

Informacje kontaktowe

Profil użytkownika

Adres e-mail

W kontakcie

19 znakowa nazwa użytkownika

E-mail wysłany

Na adres

wysłaliśmy Ci e-maila z linkiem, który
umożliwi odzyskanie dostępu do konta.

OK

a*****1@domena.com
9 znakowa nazwa użytkownika



E-mail służbowy – według schematu firmowego

imie.nazwisko@nokia.com

Welcome to your link to getting the email address format for employees at **NSN - Nokia Solutions and Networks**.

Our site is designed for people who don't have the massive budget for enterprise sales and marketing data. When you know who to reach out to but not their address - then Email Format is your savior!

Don't sweat it, we've got you covered with the free data below. This is only a snapshot of the 25M+ companies included in our research.

Get the email address format for people working at

nokia.com



Identified Name Formats Representative Email Addresses Export to Excel

medium confidence

first_name . last_name	 	e.g. John.Smith@nokia.com
low confidence		
first_name last_name	 	e.g. JohnSmith@nokia.com
last_name	 	e.g. Smith@nokia.com



Numer telefonu

The screenshot shows a search interface with the following statistics at the top:

1 RESULT(S) FOUND	308MS SEARCH ELAPSED TIME	14,453,524,343 ASSETS SEARCHED	48,796 AGGREGATED DATA WELLS
----------------------	------------------------------	-----------------------------------	---------------------------------

Results:

Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.

What's DeHashed and those results?

Result
Name
Email
Hashed Password
Phone

Sourced from Morele data →
Request entry removal ↗



Praca

Doświadczenie



Nokia

1 rok 2 mies.

- **Software Tester**
maj 2022 –obecnie · 7 mies.

- **Working Student**
paź 2021 – kwi 2022 · 7 mies.



Rodzina – wujek

Związek



Brak informacji o związku do wyświetlenia

Członkowie rodziny



Wujek



Osiągnięcia sportowe

gimnazja

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]
7. [REDACTED] 99 Gim 3 Gzycko **42.58** 309

Mistrzostwa PWr w pływaniu i tenisie stołowym



amator złote medale

Gimnazja

Dziewczęta

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]
7. [REDACTED]
8. [REDACTED]
9. [REDACTED]
11. [REDACTED]
11. [REDACTED]
13. Gim 3 Gzycko 2



Osiągnięcia sportowe

Osiągnięcia uczniów I LO w Giżycku w olimpiadach, konkursach i zawodach sportowych w roku szkolnym 2017-2018

Mistrzostwa Województwa w drużynowych zawodach w pływaniu dziewcząt
Licealiada Dziewczęta Rocznik 1998 i młodsi II miejsce

Rocznik 1998 i młodsi Dziewczęta 50m klasyczny
3e II miejsce

Sztafeta 6x50m Dziewczęta Rocznik 1998 i młodsi II miejsce

3e

Finał Mistrzostw Województwa SPP w koszykówce dziewcząt V-VI miejsce

3e



Dodatkowe informacje - haveibeenpwned

The screenshot shows the homepage of haveibeenpwned. At the top, a large button reads ':--have i been pwned?'. Below it, a sub-header says 'Check if your email or phone is in a data breach'. A search bar is followed by a 'pwned?' button. The main content area has a red background and displays the message 'Oh no — pwned!' with the subtext 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. Below this, there are social media sharing icons and a 'Donate' button. A section titled 'Breaches you were pwned in' lists the 'Morele.net' breach, which occurred in October 2018, involving 2.5 million unique email addresses, names, and passwords. The 'Compromised data' listed is 'Email addresses, Names, Passwords, Phone numbers'. The Morele.net logo is shown as a red stylized 'm'.

:--have i been pwned?

Check if your email or phone is in a data breach

pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Facebook Twitter Bitcoin PayPal Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Morele.net: In October 2018, the Polish e-commerce website Morele.net suffered a data breach. The incident exposed almost 2.5 million unique email addresses alongside phone numbers, names and passwords stored as md5crypt hashes.

Compromised data: Email addresses, Names, Passwords, Phone numbers



Dodatkowe informacje - dehashed

The screenshot shows a search interface with the following statistics:

1 RESULT(S) FOUND	308MS SEARCH ELAPSED TIME	14,453,524,343 ASSETS SEARCHED	48,796 AGGREGATED DATA WELLS
----------------------	------------------------------	-----------------------------------	---------------------------------

Results:

Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.

What's DeHashed and those results?

Result	
Name	[REDACTED]
Email	[REDACTED]
Hashed Password	[REDACTED]
Phone	[REDACTED]

Sourced from Morele data

[Request entry removal ↗](#)



Dodatkowe informacje – numer telefonu

Pierwotna sieć:

Jaka to sieć - Sprawdź w jakiej sieci jest numer

Tu także sprawdzisz czy numer zmieniał operatora.

Wpisz numer i sprawdź operatora

Sprawdź

Wpisz numer komórkowy (9cyfr) np.
500600700

Numer pierwotnie przydzielony do: **Polkomtel (Plus)**

Teraz zobacz w jakiej sieci jest obecnie ten numer

Sprawdź tu

Aktualna sieć:

Tu sprawdzisz w jakiej sieci jest obecnie numer

Wyszukiwarka obsługiwana przez UKE

przez samych przedsiębiorców telekomunikacyjnych. Jeżeli procesowanie przeniesienia wprowadzonego numeru telefonu było przed datami wymienionymi powyżej i wynik wyszukiwania wskazuje na niewłaściwego dostawcę usług, należy w takim przypadku zwrócić się do swojego dostawcy z prośbą o podjęcie działań zmierzających do dokonania w bazie korekty.

Wyszukiwanie Dostawcy usług dla danego numeru telefonu jest aktualne na dzień wyszukiwania. Dane zmieniają się raz na dobę w nocy.

Wpisz numer

Nie jestem robotem



reCAPTCHA
Prywatność - Warunki

Znajdź

Operatorem numeru **jest T-MOBILE POLSKA S.A. (RPT: 4)**

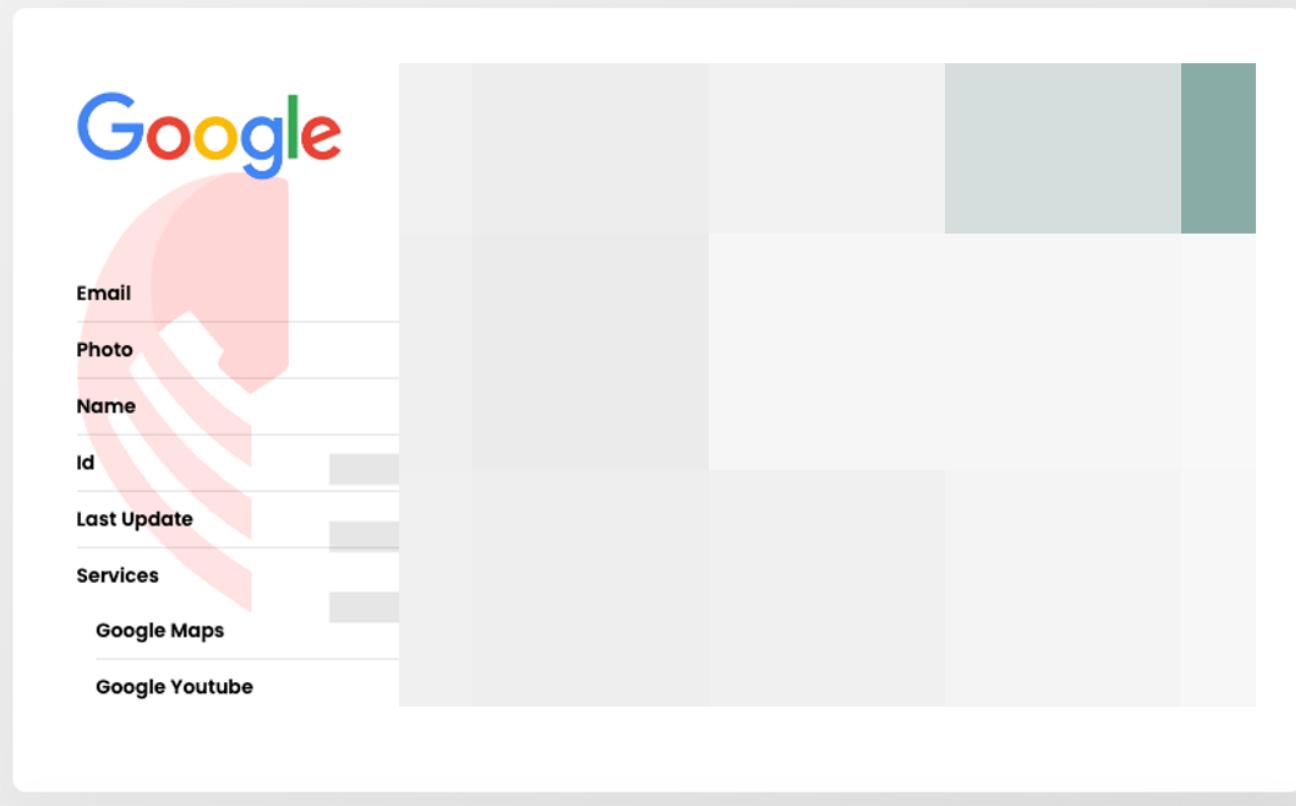


Dodatkowe informacje – konto skype



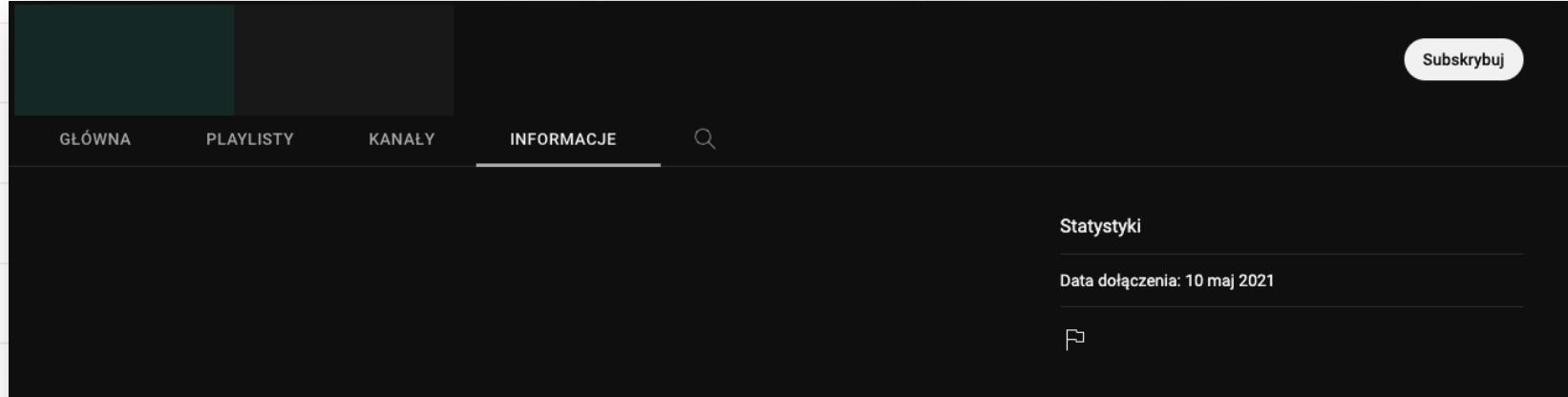


Dodatkowe informacje – konto google

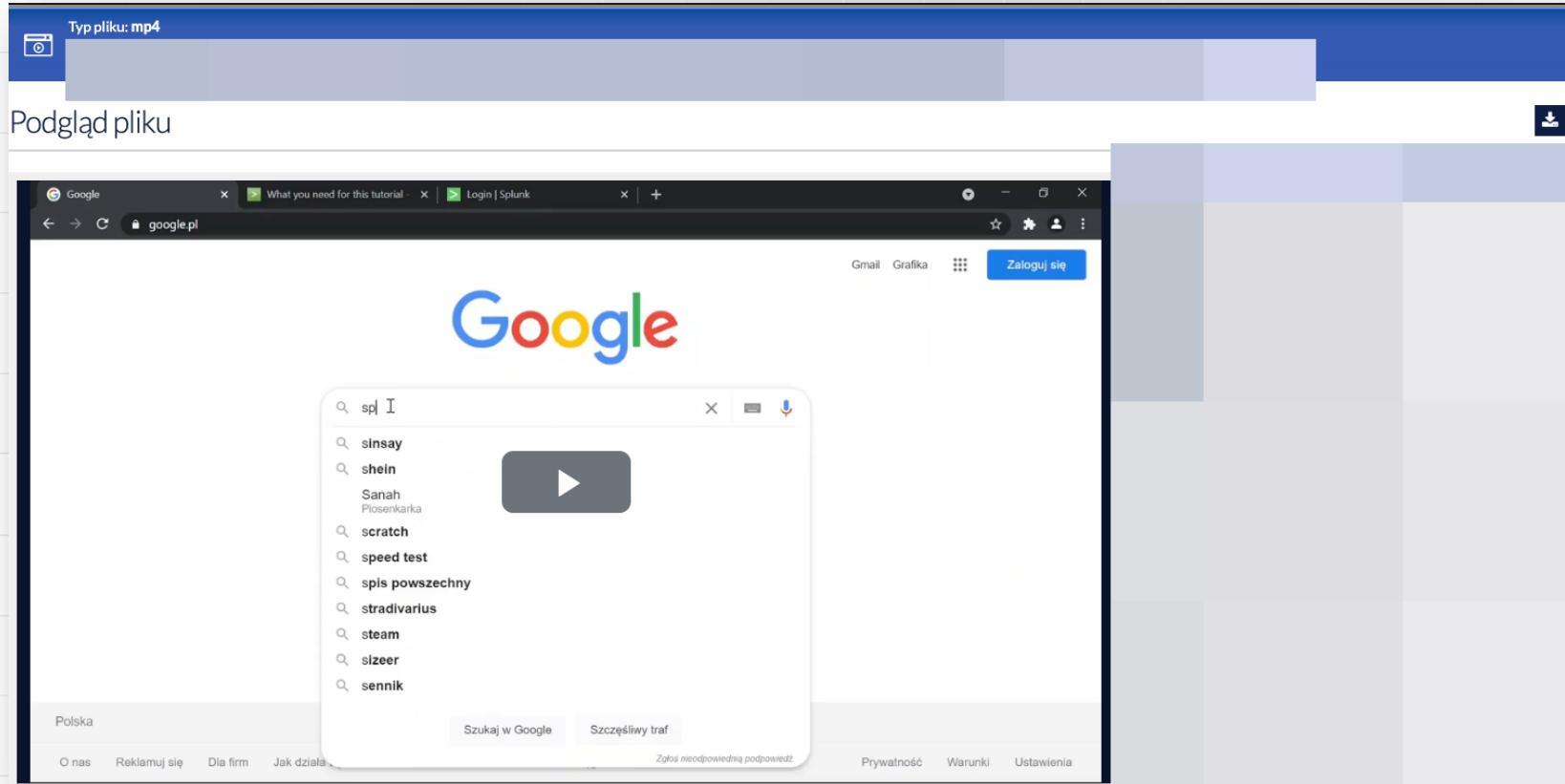




Dodatkowe informacje – konto youtube

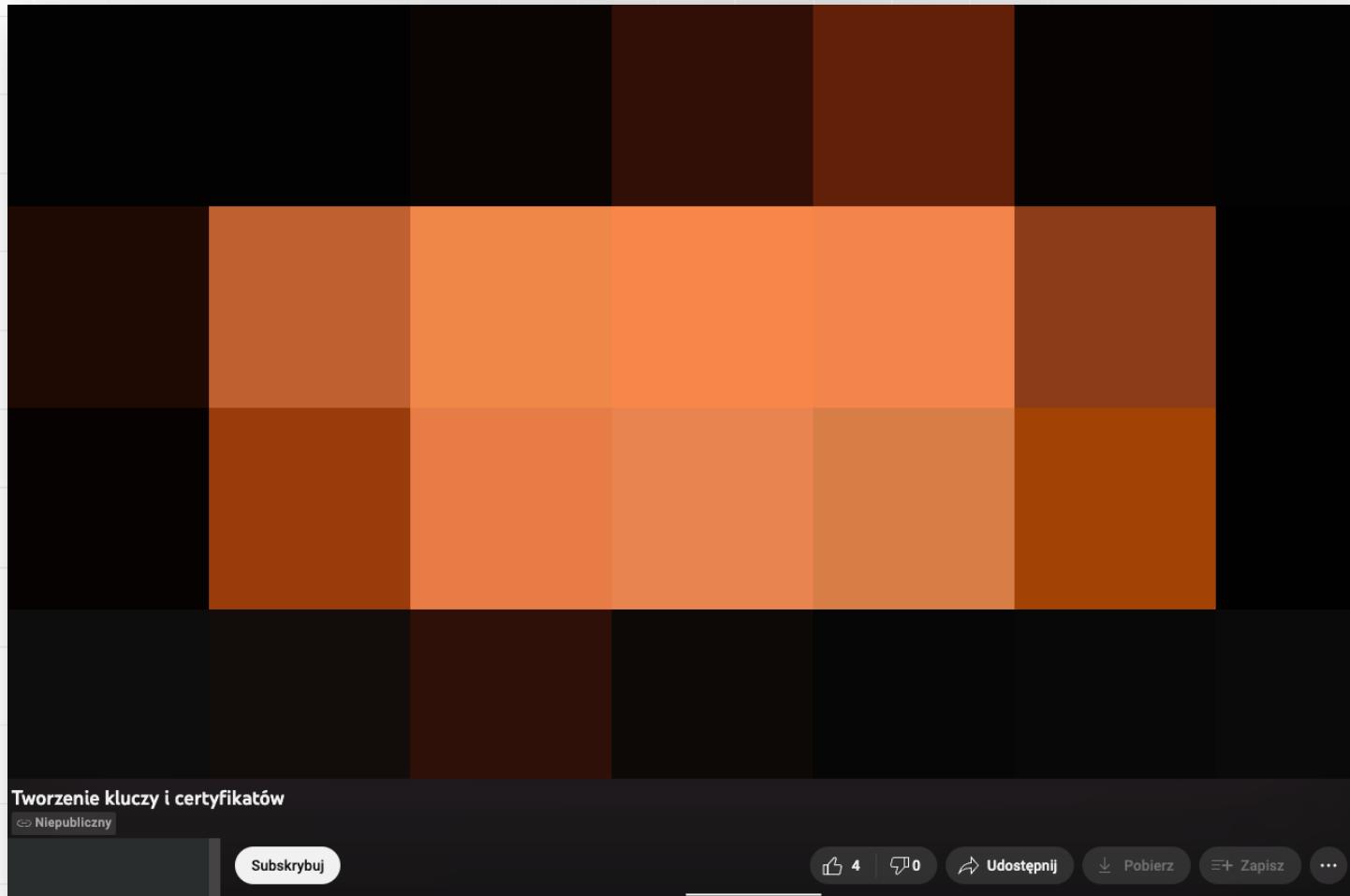


Dodatkowe informacje – nagrania wideo z głosem ofiary





Dodatkowe informacje – nagrania wideo z głosem ofiary





Social engineering



Standardowy proces logowania - zoom

Planowany termin zdalnych zajęć Seminarium kierunkowe - Seminarium Odebrane x



J

przez e-science.pl

paź	Seminarium kierunkowe Kiedy czw. 20 paź 2022 3:15pm – 4:55pm (CEST) Kto [REDACTED] Dodaj do kalendarza »	Plan dnia czw. 20 paź 2022 <i>Brak wcześniejszych wydarzeń</i> 3:15pm Seminarium kierunkowe <i>Brak późniejszych wydarzeń</i>
-----	--	--

For English scroll down.

Szanowni Państwo!

Zajęcia z Seminarium kierunkowe w terminie 20 października 2022 15:15 odbędą się za pomocą systemu telekonferencyjnego.

Link do spotkania:

<https://pwr-edu.zoom.us/j/99200062036?pwd=c095c05PWfhSDUSSkIPazJDMTJJUT09>

hasło: TWuCEG

Połączenie możliwe jest z systemów operacyjnych Windows, Linux, MacOS oraz urządzeń mobilnych Android i iOS.

W celu uczestnictwa proszę:

1. Otworzyć powyższy link;
2. Postępować zgodnie z wyświetlona instrukcją - zainstalować klienta jeżeli nie jest zainstalowany lub pobrać ze sklepu Google Play lub Android Store;

3. Wybrać "Sign in to Join";

4. Kliknąć przycisk "Sign in with SSO";
UWAGA: Nie należy wpisywać adresu e-mail i hasła w oknie aplikacji Zoom. Logujemy się wyłącznie poprzez stronę PWr.

5. Podać adres SSO pwr-edu.zoom.us - przeglądarka zostanie przekierowana na stronę PWr;
UWAGA: Wykorzystanie mechanizmu institutional sso do uwierzytelniania w usłudze Zoom zapewnia, iż poświadczenie (login i hasło) nie opuszcza infrastruktury PWr.
6. Kliknąć przycisk "Nowy system uwierzytelniania" i zalogować się (jeżeli nie będzie to możliwe, zresetować hasło przy pomocy opcji "Zapomniałeś hasła?");
UWAGA: W przypadku studentów można również użyć przycisku "Google", następnie zalogować się używając loginu i hasła jak do poczty.



Standardowy proces logowania - zoom

The screenshot shows a web browser window with the title "Launch Meeting - Zoom". The URL in the address bar is "pwr-edu.zoom.us/j/99200062036?pwd=c095c05PWfhdsU1SSklPazJDMTJJUT09#success". A cookie consent dialog box is prominently displayed in the center of the page. The dialog has a title "Otworzyć zoom.us.app?", a message about opening the application, and a checkbox asking for permission to always open such links. At the bottom are three buttons: "Anuluj" (Cancel), "Otwórz zoom.us.app" (Open zoom.us.app), and two blue buttons for cookie preferences: "USTAWIENIA PLIKÓW COOKIE" (Cookie Settings) and "AKCEPTUJ PLIKI COOKIE" (Accept Cookies). Below the dialog, there is a note about the Zoom Client and links to download it or join from the browser.

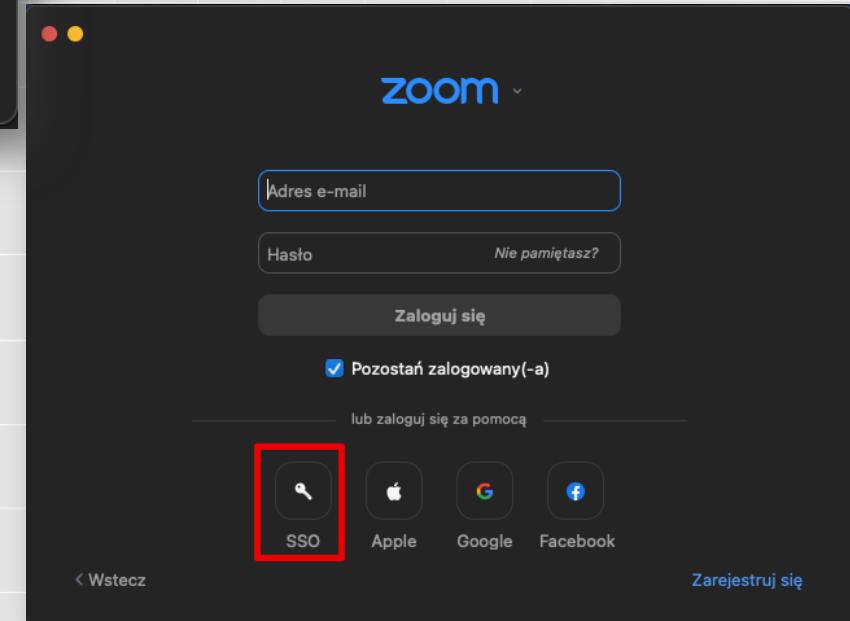
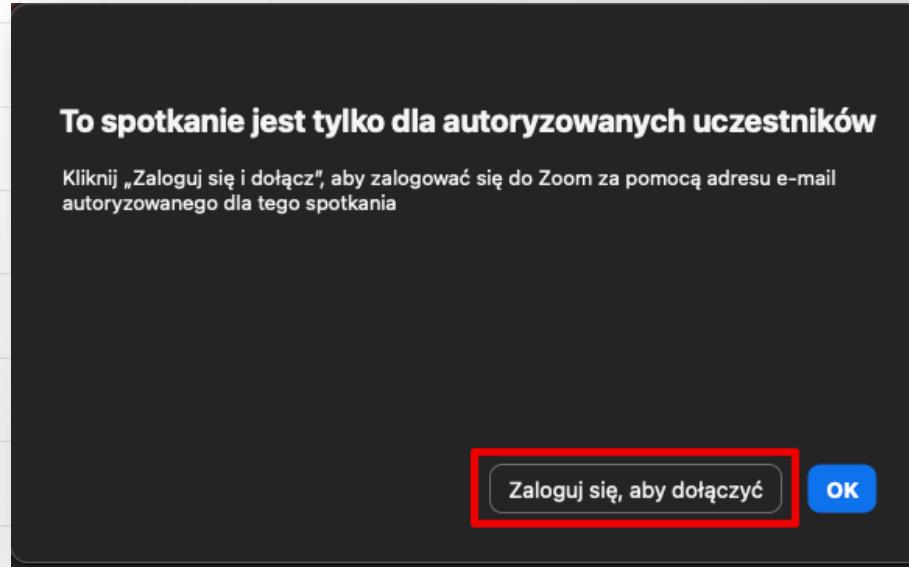
Don't have Zoom Client installed? [Download Now](#)

Having issues with Zoom Client? [Join from Your Browser](#)

©2022 Zoom Video Communications, Inc. All rights reserved.
[Privacy & Legal Policies](#) | [Do Not Sell My Personal Information](#) | [Cookie Preferences](#)

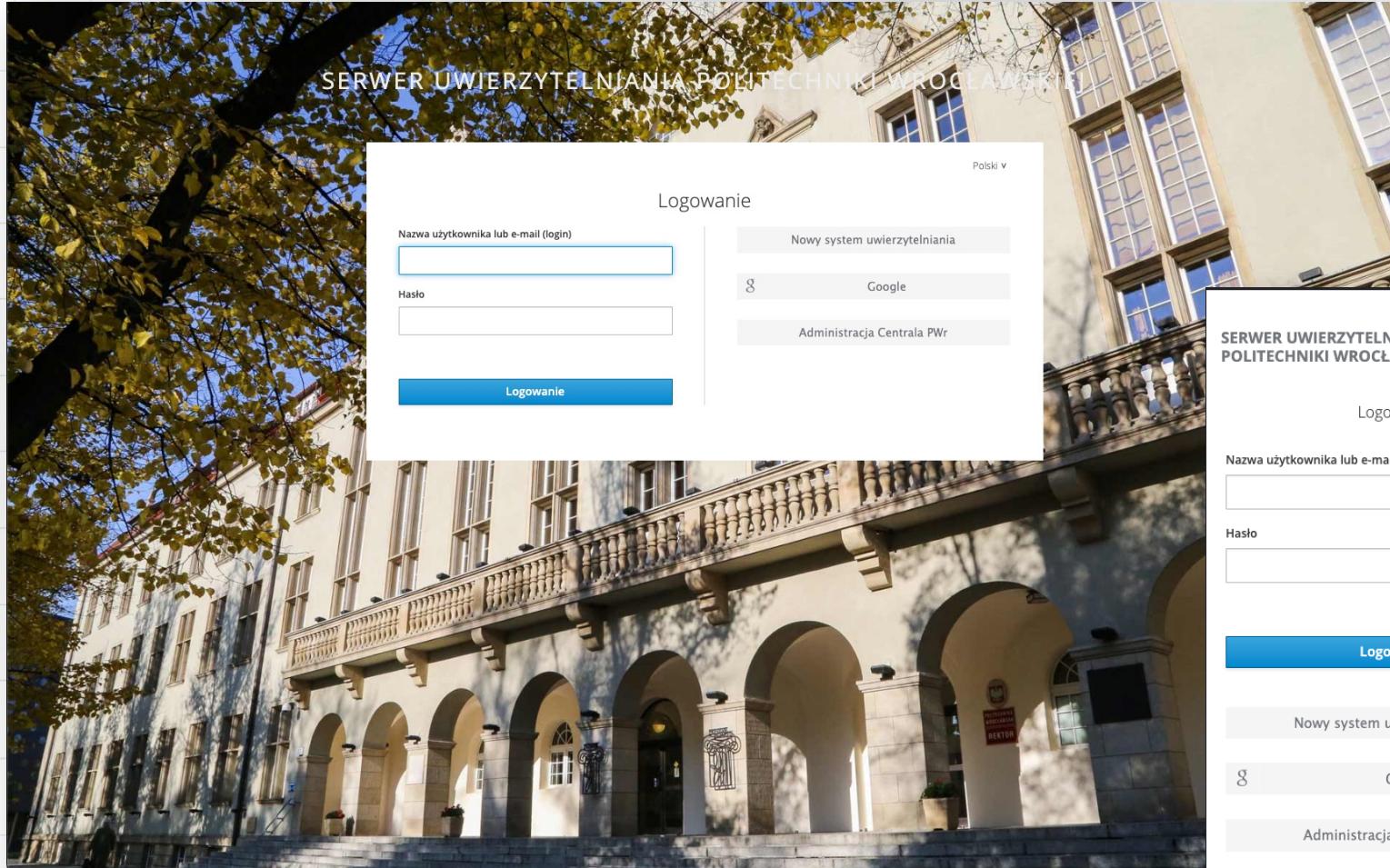
pwr-edu.zoom.us/

Standardowy proces logowania - zoom





Standardowy proces logowania - zoom



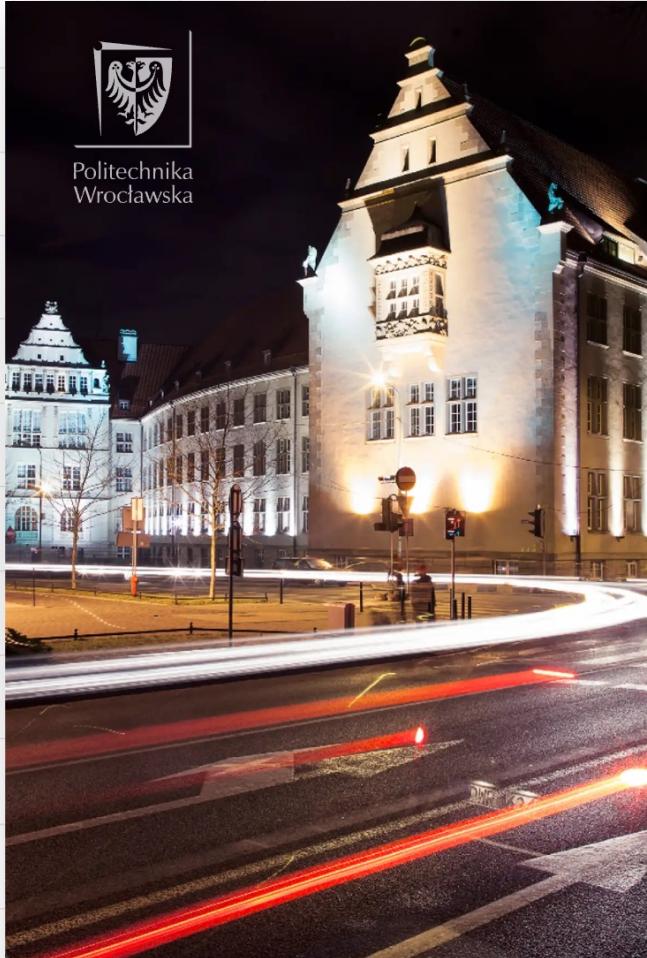
kc.e-science.pl/

wersja moblina →



Politechnika
Wrocławska

Standardowy proces logowania - zoom



Politechnika
Wrocławska



Politechnika Wrocławska

Witaj w systemie logowania

Polski



Nazwa użytkownika



Hasło

Zaloguj

Wyczść

[Nie pamiętam hasła](#)

System logowania pozwala na dostęp do usług informatycznych Politechniki Wrocławskiej. Użyj nazwy użytkownika i hasła z systemu Active Directory. Jeżeli nie znasz nazwy użytkownika lub hasła użyj opcji Nie pamiętam hasła.

W przypadku problemu z logowaniem napisz na adres pomoc+konto@pwr.edu.pl.

Politechnika Wrocławska © 2022
Wrocławskie Centrum Sieciowo-Superkomputerowe

login.pwr.edu.pl/

wersja moblina →



Politechnika Wrocławska

Witaj w systemie logowania

Polski



Nazwa użytkownika



Hasło

Zaloguj

Wyczść

[Nie pamiętam hasła](#)

System logowania pozwala na dostęp do usług informatycznych Politechniki Wrocławskiej. Użyj nazwy użytkownika i hasła z systemu Active Directory. Jeżeli nie znasz nazwy użytkownika lub hasła użyj opcji Nie pamiętam hasła.

W przypadku problemu z logowaniem napisz na adres pomoc+konto@pwr.edu.pl.

Politechnika Wrocławska © 2022
Wrocławskie Centrum Sieciowo-Superkomputerowe



Standardowy proces logowania - zoom

Zaloguj się
Przejdz do aplikacji WCSS-ZOOM

Wpisz swój adres e-mail @student.pwr.edu.pl

Nie pamiętasz adresu?

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

Utwórz konto Dalej

Zaloguj się
Przejdz do aplikacji WCSS-ZOOM

Wpisz swój adres e-... @student.pwr.edu.pl

Nie pamiętasz adresu?

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

Utwórz konto Dalej

Witamy
@student.pwr.edu.pl

Wpisz hasło

Pokaż hasło

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

Nie pamiętasz hasła? Dalej

polski ▾

Zaloguj się przez Google

Witamy
@student.pwr.edu.pl

Wpisz hasło

Pokaż hasło

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

Nie pamiętasz hasła? Dalej

polski ▾ Pomoc Prywatność Warunki

↑ wersja mobilna ↑



Phishingowy proces logowania - zoom

Jakub Tomaszewski jakub.tomaszewski@pwr.edu.pl przez sendinblue.com
do mnie ▾

Szanowni Państwo!

Dzisiejsze zajęcia projektowe wyjątkowo dzisiaj odbędą się na platformie zoom.

Link do zajęć wyśle w osobnej wiadomości. Obecność obowiązkowa!

Pozdrawiam,

JT.

czw., 27 paź, 16:39 (9 dni temu) ⚡ ↗ ⋮

Planowany termin zdalnych zajęć Zaawansowane Testy Penetracyjne - Projekt Odebrane x

Jakub Tomaszewski jakub.tomaszewski@pwr.edu.pl przez sendinblue.com
do mnie ▾

paź 17 pon. ▾

Zaawansowane testy penetracyjne

Kiedy pon. 17 paź 2022 5:05pm – 7:40pm (CEST)
Kto Jakub Tomaszewski*

[Dodaj do kalendarza »](#)

Plan dnia

pon. 17 paź 2022

Brak wcześniejszych wydarzeń

5:05pm Zaawansowane testy penetracyjne

Brak późniejszych wydarzeń

czw., 27 paź, 16:35 (9 dni temu) ⚡ ↗ ⋮

For English scroll down.

Szanowni Państwo!

Zajęcia z Zaawansowanymi Testów Penetracyjnych w terminie 27 października 2022 17:05 odbędą się za pomocą systemu telekonferencyjnego.

Link do spotkania:

<https://pwr-edu.zoom.us/j/97756133274&pwd=OGEyNFhtdhkczdpMld6cJRYnE1QT09&success/>

hasło: E6Ta6e

Połączenie możliwe jest z systemów operacyjnych Windows, Linux, MacOS oraz urządzeń mobilnych Android i iOS.

W celu uczestnictwa proszę:

1. Otworzyć powyższy link;
2. Postępować zgodnie z wyświetlona instrukcją - zainstalować klienta jeżeli nie jest zainstalowany lub pobrać ze sklepu Google Play lub Android Store;
3. Wybrać "Sign in to Join";
4. Kliknąć przycisk "Sign in with SSO";
UWAGA: Nie należy wpisywać adresu e-mail i hasła w oknie aplikacji Zoom. Logujemy się wyłącznie poprzez stronę PWr.
5. Podać adres SSO pwr-edu.zoom.us - przeglądarka zostanie przekierowana na stronę PWr;
UWAGA: Wykorzystanie mechanizmu institutionalnego sso do uwierzytelniania w usłudze Zoom zapewnia, iż poświadczenie (login i hasło) nie opuszcza infrastruktury PWr.
6. Kliknąć przycisk "Nowy system uwierzytelniania" i zalogować się (jeżeli nie będzie to możliwe, zresetować hasło przy pomocy opcji "Zapomniałeś hasła?");
UWAGA: W przypadku studentów można również użyć przycisku "Google", następnie zalogować się używając loginu i hasła jak do poczty.
7. Wybrać "Join using computer audio" - w przypadku braku mikrofonu można wykorzystać połączenie telefoniczne, informacje w zakładce "Call in";



Phishingowy proces logowania - zoom

The screenshot shows a browser window with the following details:

- Title Bar:** Uruchom spotkanie - Zoom
- URL:** pwr-edu.zooom.edu.pl/j/97756133274&pwd=OGEyNFhtdnhkczdpMld6clJRYnE1QT09&success/
- Content Area:**
 - Header:** Komunikat ze strony pwr-edu.zooom.edu.pl
 - Text:** Otwórz aplikację zoom.us.app?
 - Buttons:** Anuluj (grey) and OK (blue)
- Message:** Kliknij **Otwórz zoom.us** w oknie dialogowym wyświetlonym w przeglądarce
Jeśli nie widzisz okna dialogowego, kliknij **Uruchom spotkanie** poniżej
- Acceptance Text:** Klikając „Uruchom spotkanie”, akceptujesz nasze [Warunki świadczenia usług](#) i [Oświadczenie o prywatności](#)
- Call-to-Action:** Uruchom spotkanie (blue button)
- Bottom Links:** Nie masz jeszcze zainstalowanego klienta stacjonarnego Zoom? [Pobierz teraz](#)
Masz problemy z klientem stacjonarnym Zoom? [Dołącz z przeglądarki](#)
- Footer:** ©2022 Zoom Video Communications, Inc. Wszystkie prawa zastrzeżone.
Polityki prawna i prywatności | Nie sprzedawaj moich danych osobowych | Preferencje systemowe



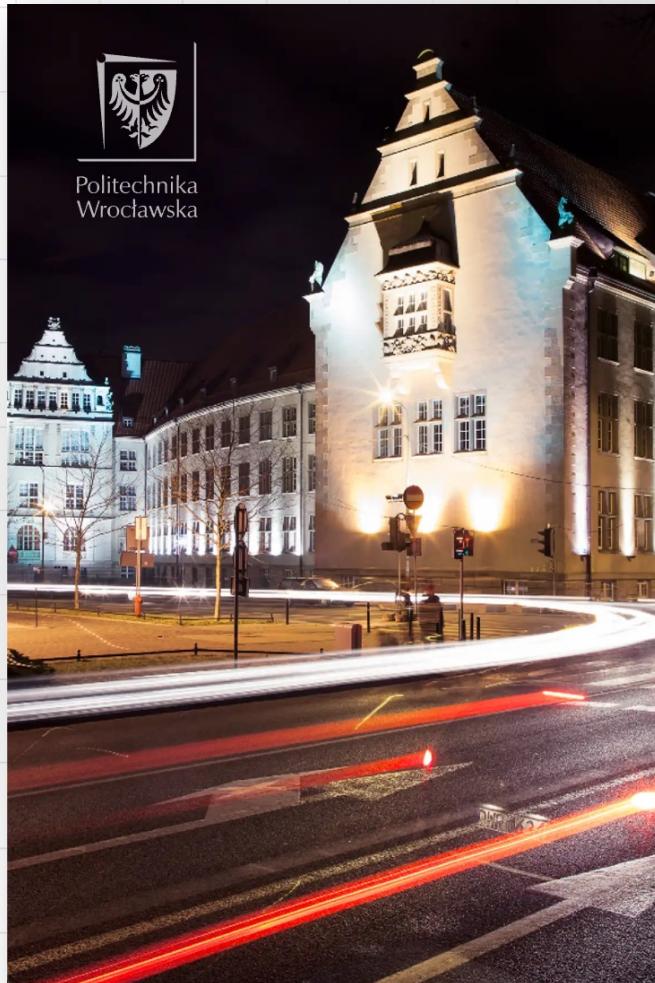
Phishingowy proces logowania - zoom

The image illustrates a phishing attack targeting the University of Wrocław. On the left, a photograph of the university's classical building is overlaid with two screenshots of a phishing website. The top screenshot shows a desktop view where the background image of the building is very large, covering most of the page. The bottom screenshot shows a mobile or tablet view where the background image is much smaller and centered. Both screenshots show a login form for 'SERWER UWIERZYTELNIANIA POLITECHNIKI WROCŁAWSKIEJ' (Authentication Server of the University of Wrocław). The forms include fields for 'Nazwa użytkownika lub e-mail (login)' and 'Hasło', and a 'Logowanie' button. Below the button are links for 'Nowy system uwierzytelniania', 'Google', and 'Administracja Centralna PWr'. The mobile version has a 'Polski v' link at the top right.

wersja moblina →



Phishingowy proces logowania - zoom



Witaj w systemie logowania

Polski ▾

Nazwa użytkownika

Hasło

Zaloguj

Wyczysć

Nie pamiętam hasła

System logowania pozwala na dostęp do usług informatycznych Politechniki Wrocławskiej. Użyj nazwy użytkownika i hasła z systemu Active Directory. Jeżeli nie znasz nazwy użytkownika lub hasła użyj opcji Nie pamiętam hasła.

W przypadku problemu z logowaniem napisz na adres pomoc+konto@pwr.edu.pl

wersja moblina →



Witaj w systemie logowania

Polski ▾

Nazwa użytkownika

Hasło

Zaloguj

Wyczysć

Nie pamiętam hasła

System logowania pozwala na dostęp do usług informatycznych Politechniki Wrocławskiej. Użyj nazwy użytkownika i hasła z systemu Active Directory. Jeżeli nie znasz nazwy użytkownika lub hasła użyj opcji Nie pamiętam hasła.

W przypadku problemu z logowaniem napisz na adres pomoc+konto@pwr.edu.pl



Phishingowy proces logowania - zoom

Google

Zaloguj się

Przejdz do aplikacji [WCSS-ZOOM](#)

Wpisz swój adres email @student.pwr.edu.pl

Nie pamiętasz adresu?

Aby można było przejść dalej, Google udostępnii aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

[Utwórz konto](#)

polski ▾

Google

@student.pwr.edu.pl

Wpisz hasło

Pokaż hasło

Aby można było przejść dalej, Google udostępnii aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

Nie pamiętasz hasła? [Dalej](#)

polski ▾ [Pomoc](#) [Prywatność](#) [Warunki](#)

Google

Zaloguj się

Przejdz do aplikacji [WCSS-ZOOM](#)

Wpisz swój adres email @student.pwr.edu.pl

Nie pamiętasz adresu?

Aby można było przejść dalej, Google udostępnii aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

[Utwórz konto](#) [Dalej](#)

Pokaż hasło

Aby można było przejść dalej, Google udostępnii aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

Nie pamiętasz hasła? [Dalej](#)

Pomoc Prywatność Warunki ▾

↑ wersja mobilna ↑



Porównanie procesów logowania - google

Zaloguj się

Przejdz do aplikacji [WCSS-ZOOM](#)

Wpisz swój adres e-mail @student.pwr.edu.pl

[Nie pamiętasz adresu?](#)

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

[Utwórz konto](#) [Dalej](#)

Google

Zaloguj się

Przejdz do aplikacji [WCSS-ZOOM](#)

Wpisz swój adres email @student.pwr.edu.pl

[Nie pamiętasz adresu?](#)

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

[Utwórz konto](#) [Dalej](#)

polski ▾

Zaloguj się przez Google

Witamy

@student.pwr.edu.pl

Wpisz hasło

Pokaż hasło

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

[Nie pamiętasz hasła?](#) [Dalej](#)

polski ▾

Pomoc Prywatność Warunki

polski ▾

Google

Wpisz hasło

Pokaż hasło

Aby można było przejść dalej, Google udostępnia aplikacji WCSS-ZOOM Twoją nazwę użytkownika, adres e-mail, ustawienia języka i zdjęcie profilowe.

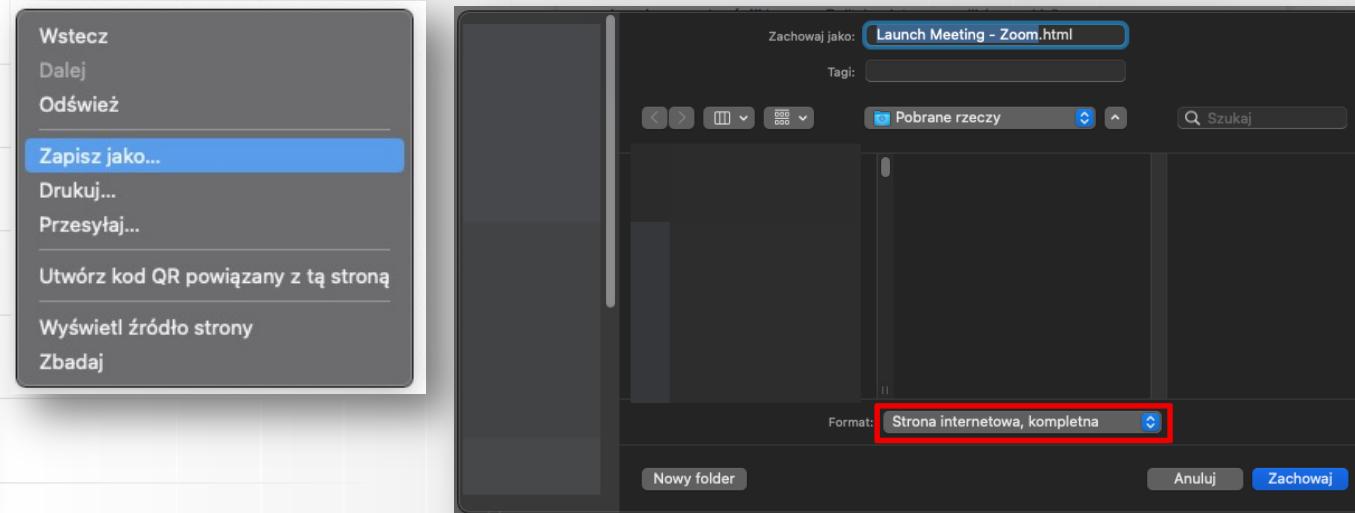
[Nie pamiętasz hasła?](#) [Dalej](#)

polski ▾

Pomoc Prywatność Warunki

Scenariusz ataku phishingowego

Tworzenie stron phishingowych:



<https://github.com/dmdhruvilmistry/GooglePhish>

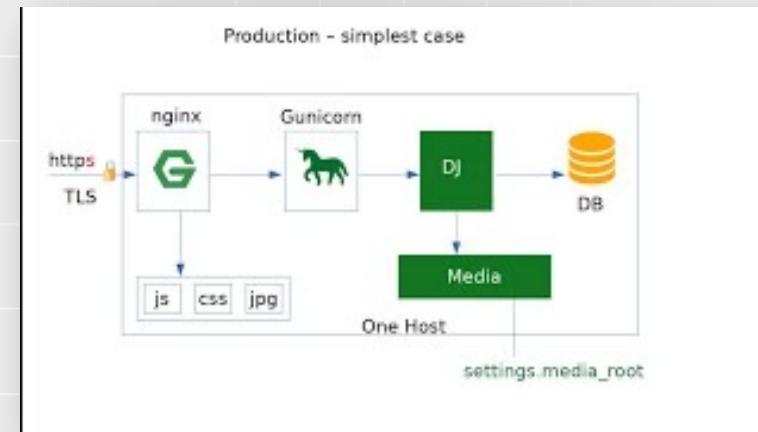


Scenariusz ataku phishingowego

3 maszyny wirtualne hostujące 3 witryny:

Stan	Nazwa ↑	Strefa	Zalecenia	Używany przez
✓	google	us-west4-b	💡 Oszczędź 13 \$/miesiąc	
✗	instance-1	us-west4-b		
✓	kce	us-west4-b	💡 Oszczędź 25 \$/miesiąc 💡 Oszczędź 13 \$/miesiąc	
✓	zooom	us-west4-b	💡 Oszczędź 13 \$/miesiąc	

każda maszyna zawierała aplikację napisaną w języku Python z użyciem framework'a Django hostowaną za pomocą gunicorn oraz Nginx z certyfikatem od Let's encrypt. Każda instancja zawierała bazę sqlite





Scenariusz ataku phishingowego

Certyfikat SSL:

Przeglądarka certyfikatów: pwr-edu.zooom.edu.pl

X

Ogólne Szczegóły

Wystawiony dla

Nazwa pospolita (CN)	pwr-edu.zooom.edu.pl
Organizacja (O)	<brak w certyfikacie>
Jednostka organizacyjna (OU)	<brak w certyfikacie>

Wystawiony przez

Nazwa pospolita (CN)	R3
Organizacja (O)	Let's Encrypt
Jednostka organizacyjna (OU)	<brak w certyfikacie>

Okres ważności

Wystawiony dnia	wtorek, 25 października 2022 21:23:59
Wygasa dnia	poniedziałek, 23 stycznia 2023 20:23:58

Odciski cyfrowe

Odcisk cyfrowy SHA-256	4C AC 36 BC EB 74 6E 51 8C 74 E3 56 75 98 B0 58 A8 C1 C1 96 85 22 BE 25 58 29 D2 45 50 91 46 D4
Odcisk cyfrowy SHA-1	9F FB 29 64 DD B0 42 43 A8 AE E5 ED 53 15 64 46 A3 F4 F3 1B



Scenariusz ataku phishingowego

Sprawdzenie terminu zajęć grupy, do której zapisana jest ofiara:

K05-81c	CBEU00301P Mgr inż. Jakub Tomaszewski cz 17:05-19:40, bud. C-1, sala sala wirtualna	Zaawans. testy penetracyjne .. Projekt Szczegółowy terminarz
K05-81d	CBEU00301P dr inż. Michał Walkowski cz 18:00-20:35, bud. C-1, sala sala wirtualna	Zaawans. testy penetracyjne .. Projekt Szczegółowy terminarz

Wiadomość informująca o zmianie miejsca zajęć (prowadzący zazwyczaj prowadzi zajęcia na platformie google meet):

```
(kali㉿kali)-[~]
└─$ sudo sendemail -xu [REDACTED] -xp [REDACTED] -s smtp-relay.sendinblue.com:587 -f "Jakub Tomaszewski <jakub.tomaszewski@pwr.edu.pl>" -t "[REDACTED]@student.pwr.edu.pl" -u "ZMIANA MIEJSCA ZAJĘC Zaawansowane testy penetracyjne - Projekt" -o message-file=email2.txt -o message charset="utf-8"
```

Wiadomość z linkiem do strony phishingowej:

```
(kali㉿kali)-[~]
└─$ sudo sendemail -xu [REDACTED] -xp [REDACTED] -s smtp-relay.sendinblue.com:587 -f "Jakub Tomaszewski <jakub.tomaszewski@pwr.edu.pl>" -t "[REDACTED]@student.pwr.edu.pl" -u "Planowany termin zdalnych zajęć Zaawansowane Testy Penetracyjne - Projekt" -o message-file=email.txt -o message charset="utf-8" -a ical.ics
```



Scenariusz ataku phishingowego

Jakub Tomaszewski jakub.tomaszewski@pwr.edu.pl przez sendinblue.com do mnie ▾

Szanowni Państwo!

Dzisiajsze zajęcia projektowe wyjątkowo dzisiaj odbędą się na platformie zoom.

Link do zajęć wyśle w osobnej wiadomości. Obecność obowiązkowa!

Pozdrawiam,

JT.

czw., 27 paź, 16:39 (9 dni temu) ⭐ ↵ ⋮

Planowany termin zdalnych zajęć Zaawansowane Testy Penetracyjne - Projekt Odebrane x

Jakub Tomaszewski jakub.tomaszewski@pwr.edu.pl przez sendinblue.com do mnie ▾

paź 17 pon.

Zaawansowane testy penetracyjne

Kiedy pon. 17 paź 2022 5:05pm – 7:40pm (CEST)
Kto Jakub Tomaszewski*
[Dodaj do kalendarza »](#)

Plan dnia
pon. 17 paź 2022
Brak wcześniejszych wydarzeń
5:05pm Zaawansowane testy penetracyjne
Brak późniejszych wydarzeń

For English scroll down.

Szanowni Państwo!

Zajęcia z Zaawansowanych Testów Penetracyjnych w terminie 27 października 2022 17:05 odbędą się za pomocą systemu telekonferencyjnego.

Link do spotkania:

<https://pwr-edu.zoom.us/j/97756133274&pwd=OGEyNFhtdhkczdpMld6clJRYnE1QT09&success/>

hasło: E6Ta6e

Połączenie możliwe jest z systemów operacyjnych Windows, Linux, MacOS oraz urządzeń mobilnych Android i iOS.

W celu uczestnictwa proszę:

1. Otworzyć powyższy link;
2. Postępować zgodnie z wyświetlona instrukcją - zainstalować klienta jeżeli nie jest zainstalowany lub pobrać ze sklepu Google Play lub Android Store;
3. Wybrać "Sign in to Join";
4. Kliknąć przycisk "Sign in with SSO";
UWAGA: Nie należy wpisywać adresu e-mail i hasła w oknie aplikacji Zoom. Logujemy się wyłącznie poprzez stronę PWr.
5. Podać adres SSO pwr-edu.zoom.us - przeglądarka zostanie przekierowana na stronę PWr;
UWAGA: Wykorzystanie mechanizmu institutionalnego sso do uwierzytelniania w usłudze Zoom zapewnia, iż poświadczenie (login i hasło) nie opuszcza infrastruktury PWr.
6. Kliknąć przycisk "Nowy system uwierzytelniania" i zalogować się (jeżeli nie będzie to możliwe, zresetować hasło przy pomocy opcji "Zapomniałeś hasła?");
UWAGA: W przypadku studentów można również użyć przycisku "Google", następnie zalogować się używając loginu i hasła jak do poczty.
7. Wybrać "Join using computer audio" - w przypadku braku mikrofonu można wykorzystać połączenie telefoniczne, informacje w zakładce "Call in";



Scenariusz ataku phishingowego

5:34 PM ⓘ

ZMIANA MIEJSCA ZAJEC
Zaawansowane testy
penetracyjne - Projekt Odebrane

Jakub Tomaszewski 27 paź
do mnie ▾

For English scroll down.

Szanowni Państwo!

Zajęcia z Zaawansowanych Testów Penetracyjnych w terminie 27 października 2022 17:05 odbędą się za pomocą systemu telekonferencyjnego.

Link do spotkania:

<https://pwr-edu.zoom.edu.pl/j/97756133274&pwd=OGEyNFhtdnhkczdpMld6cIJRYnE1QT09&success/>

hasło: E6Ta6e

Połączenie możliwe jest z systemów operacyjnych Windows, Linux, MacOS oraz urządzeń mobilnych Android i iOS.

W celu uczestnictwa proszę:

1. Otworzyć powyższy link;
2. Postępować zgodnie z wyświetlona instrukcją - zainstalować klienta jeżeli nie jest zainstalowany lub pobrać ze sklepu Google Play lub Android Store;
3. Wybrać "Sign in to Join";
4. Kliknąć przycisk "Sign in with SSO";
UWAGA: Nie należy wpisywać adresu e-mail i hasła w oknie aplikacji Zoom. Logujemy się wyłącznie poprzez stronę

5:34 PM ⓘ

ZMIANA MIEJSCA ZAJEC
Zaawansowane testy
penetracyjne - Projekt Odebrane

Jakub Tomaszewski 27 paź
do mnie ^

Od Jakub Tomaszewski • jakub.tomaszewski@pwr.edu.pl
Do 243343@student.pwr.edu.pl
Data 27 paź 2022, 4:38 PM
🔒 Standardowe szyfrowanie (TLS).
Zobacz dane zabezpieczeń

For English scroll down.

Szanowni Państwo!

Zajęcia z Zaawansowanych Testów Penetracyjnych w terminie 27 października 2022 17:05 odbędą się za pomocą systemu telekonferencyjnego.

Link do spotkania:

<https://pwr-edu.zoom.edu.pl/j/97756133274&pwd=OGEyNFhtdnhkczdpMld6cIJRYnE1QT09&success/>

hasło: E6Ta6e

Połączenie możliwe jest z systemów operacyjnych Windows, Linux, MacOS oraz urządzeń mobilnych Android i iOS.

5:34 PM ⓘ

ZMIANA MIEJSCA ZAJEC
Zaawansowane testy
penetracyjne - Projekt Odebrane

Jakub Tomaszewski 27 paź
do mnie ^

Od Jakub Tomaszewski • jakub.tomaszewski@pwr.edu.pl
D D
D Szczegóły zabezpieczeń
Wysłane z: gy.d.sender-sib.com
Podmiot podpisujący: sendinblue.com
Bezpieczeństwo: 🔒 Standardowe
szfrowanie (TLS). Więcej informacji

For English scroll down.

Szanowni Państwo!

Zajęcia z Zaawansowanych Testów Penetracyjnych w terminie 27 października 2022 17:05 odbędą się za pomocą systemu telekonferencyjnego.

Link do spotkania:

<https://pwr-edu.zoom.edu.pl/j/97756133274&pwd=OGEyNFhtdnhkczdpMld6cIJRYnE1QT09&success/>

hasło: E6Ta6e

Połączenie możliwe jest z systemów operacyjnych Windows, Linux, MacOS oraz urządzeń mobilnych Android i iOS.



Scenariusz ataku phishingowego

Przewidywanie przyszłości. Gdy ofiara podała swój numer indeksu w spreparowanym formularzu logowania google po przejściu do sekcji wpisywania hasła zostało wyświetcone jej imię i nazwisko a gdy numer indeksu był inny niż ofiary wyświetlane było imię i nazwisko osoby znajomej ofierze.

```
email2 = email.split('@')[0]
email = email.split('@')[0] + '@student.pwr.edu.pl'
username = "Imię i nazwisko ofiary"
if email2 != 'indeks ofiary':
    username = "Imię i nazwisko osoby znajomej ofiarze"
```



Scenariusz ataku phishingowego

Aby móc dostać się do strony hostującej phishing należało przejść pod odpowiedni adres. Po wpisaniu samej nazwy domeny wyświetlała się informacja o nie znalezieniu strony (not found). Mechanizm ten pozwolił uniknąć wykrycia przez różne skrypty wyszukujące stron phishingowych, zwłaszcza dla strony z formularzem logowania google.

Nie znaleziono strony

Not Found

The requested resource was not found on this server.

Pozyskano hasła do konta studenckiego

Ofiara użyła dwóch haseł, jedno z nich było powiązane z regionem jej pochodzenia

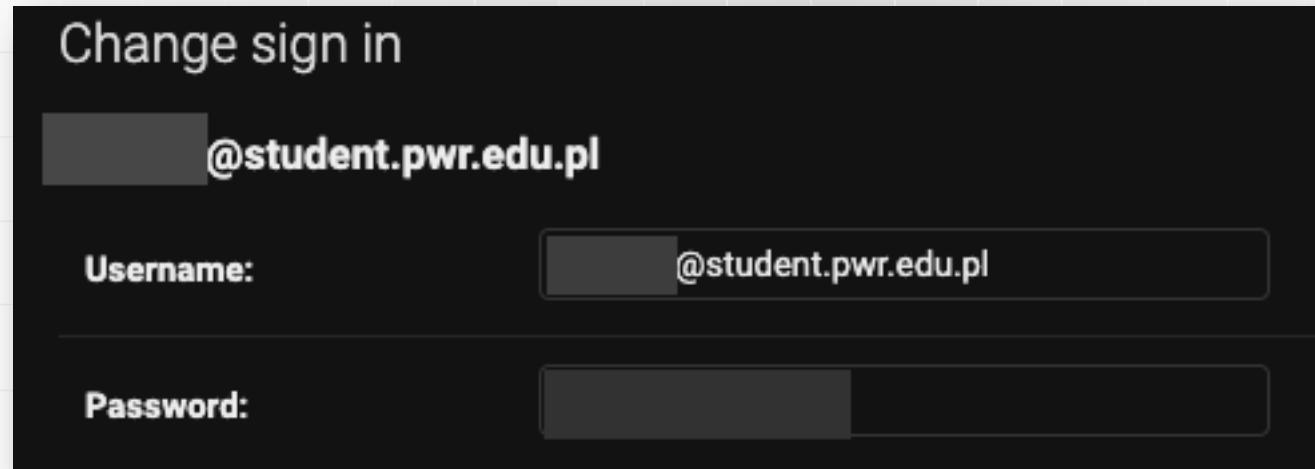
The screenshot shows the Django administration interface. The top navigation bar is blue with the text "Django administration". Below it, the breadcrumb navigation shows "Home > App > Sign ins > [REDACTED]@student.pwr.edu.pl". On the left, there's a sidebar with a search bar and sections for "APP" (containing "Sign ins" with a "+ Add" button) and "AUTHENTICATION AND AUTHORIZATION" (containing "Groups" and "Users", both with "+ Add" buttons). The main content area is titled "Change sign in" and shows a single entry for "[REDACTED]@student.pwr.edu.pl". It includes fields for "Username" (containing "[REDACTED]@student.pwr.edu.pl") and "Password" (containing two redacted fields).

The second part of the screenshot shows a dark-themed password recovery or sign-in form. At the top, it displays the email address "[REDACTED]@student.pwr.edu.pl". Below it are fields for "Username" (containing "[REDACTED]@student.pwr.edu.pl") and "Password" (containing two redacted fields).



Pozyskano hasła do konta studenckiego

dodatkowo udało się uzyskać hasło bliskiej osoby ofiary (która jednocześnie była osobą atakującą autora tej prezentacji). Hasło wyglądało jak wygenerowane przez menedżera haseł.





Lokalizacja

Pierwsza ofiara:

-- [27/Oct/2022:15:05:43 +0000] "GET

HTTP/1.1" 200

2117 "Mozilla/5.0 (Linux; Android 12; SM-G781B)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36"

geoiplookup.net Lookup IP address Prześlij

[What is my IP address](#) [IP Lookup](#) [All IP Addresses](#) [API](#)

IP Lookup for

Welcome to Geo IP Lookup, a simple yet comprehensive database of all IP addresses in the world. We started this website as an online tool anyone can use to get accurate IP address information. With us, you can find your IP address as well as input IP addresses to find details about them. Our authentic and accurate results make us the ideal website for IP information.

IP General Information

IP Address: Hostname: ISP: T-mobile Polska

IP Geolocation Information

Continent: Europe (EU) Country: Poland (PL) City: Wrocław Time Zone: Europe/Warsaw Latitude: 51.1041 (51°6'14.76" N) Longitude: 17.0348 (17°2'5.28" N)

Druga ofiara

-- [27/Oct/2022:15:09:59 +0000] "GET

HTTP/1.1" 200

2121 "Mozilla/5.0 (Linux; Android 10; EML-L29)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36"

geoiplookup.net Lookup IP address Prześlij

[What is my IP address](#) [IP Lookup](#) [All IP Addresses](#) [API](#)

IP Lookup for

Welcome to Geo IP Lookup, a simple yet comprehensive database of all IP addresses in the world. We started this website as an online tool anyone can use to get accurate IP address information. With us, you can find your IP address as well as input IP addresses to find details about them. Our authentic and accurate results make us the ideal website for IP information.

IP General Information

IP Address: Hostname: ISP: Orange Mobile

IP Geolocation Information

Continent: Europe (EU) Country: Poland (PL) City: Wrocław Time Zone: Europe/Warsaw Latitude: 51.1043 (51°6'15.48" N) Longitude: 17.0335 (17°2'0.6" N)

Geo Location



Urządzenia

Pierwsza ofiara:

-- [27/Oct/2022:15:05:43 +0000] "GET

2117 "Mozilla/5.0 (Linux; Android 12; SM-G781B)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36"

HTTP/1.1" 200

SAMSUNG GALAXY S20 FE 5G

SPECYFIKACJA TECHNICZNA



Dane	Porównaj	Testy	Aktualności	Ceny	Opinie	Pytania
Ten telefon posiada także wersję Dual SIM						
Marka	Samsung	Zobacz Smartfony Samsung				
Model	Galaxy S20 FE 5G					
Inne nazwy	SM-G781B, SM-G781N, SM-G781U, SM-G781V					
Standary	GSM, UMTS, LTE, 5G czytać więcej					
Rodzaj	Dotykowy (bez klawiatury)					
Wodo- i pyłoszczelność	IP68					
Wymiary	159.80 x 74.50 x 8.40 mm					
Waga	190.00 g					



Kup telefon w:
mediaexpert

Druga ofiara

-- [27/Oct/2022:15:09:59 +0000] "GET

2121 "Mozilla/5.0 (Linux; Android 10; EML-L29)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36"

HTTP/1.1" 200

[Home](#) / [Vendors](#) / [Huawei](#) / [P20 EML-L29](#)

HUAWEI P20 EML-L29

SPECIFICATIONS





Każdy może zostać ofiarą internetowego oszustwa. Ty (kiedyś) też.

Wiesz co to było tak że my byliśmy w galerii xd i staliśmy przy kasie na początku [REDACTED] cos tam [REDACTED] że dostaliśmy maila odnośnie zajęć z testów i [REDACTED] hasło i [REDACTED] nie wchodziło i [REDACTED] to zrobić xD raz wpisałem ale jak już wpisałem mówię kur..de

Cos jest nie tak

Patrze na tego maila dokładnie

Patrze na szyfrowanie

Aha....

niebezpiecznik.pl/kazdy



Dziękuję za uwagę 😊