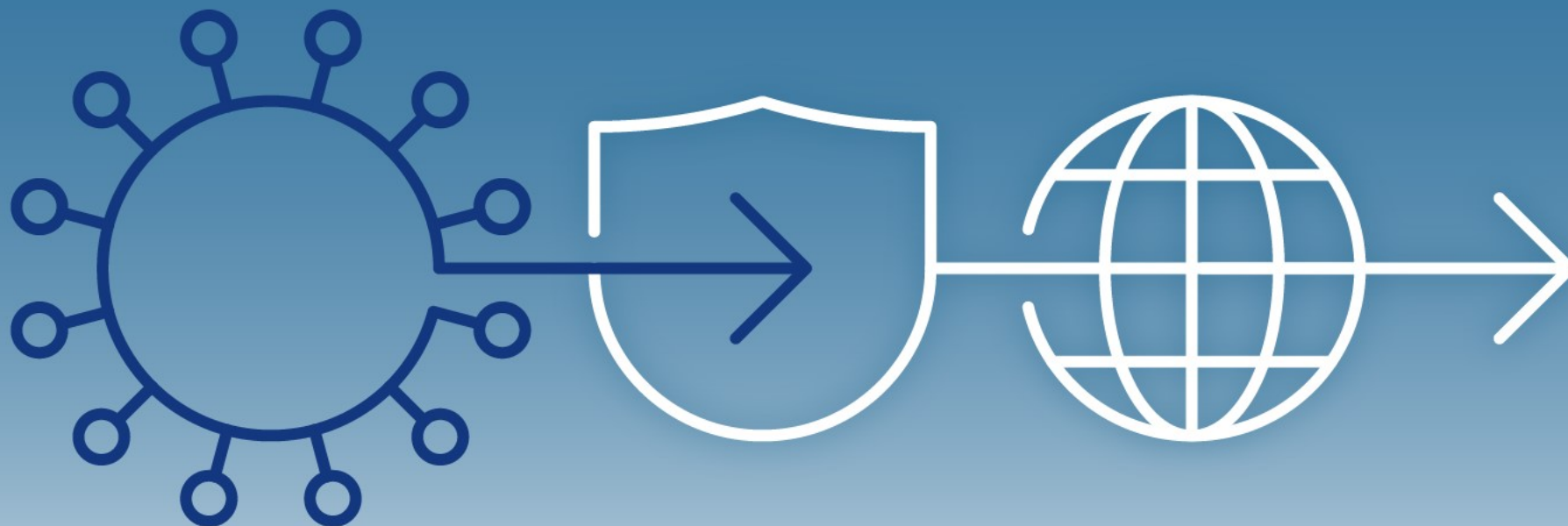


Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne

Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

Edukacja dla cyberbezpieczeństwa w czasie pandemii

Edukacyjne gry komputerowe

mgr Konrad Radomiński, mgr Wawrzyniec Święcicki, UKSW



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne

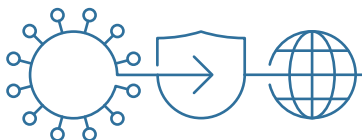
Cyberbezpieczeństwo domowników w warunkach pandemii

Jednym ze skutków pandemii jest **gwałtownie przyspieszona transformacja cyfrowa**.

Przemiana ta dotyczy większości aspektów życia codziennego – edukacji, pracy zawodowej, działalności administracji publicznej, handlu, kontaktów towarzyskich i rodzinnych oraz rozrywki.

Za przyspieszoną transformacją cyfrową **nie nadąża edukacja na temat cyberzagrożeń**.

Z powodu pandemii więcej czasu w sieci spędzają dzieci, z natury ufne i często nieświadome zagrożeń związanych z korzystaniem z Internetu. **Z tego powodu działalność cyberprzestępców stała się dużo prostrza**.

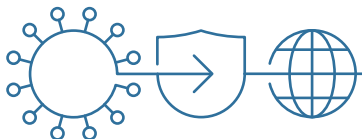


Cyberbezpieczeństwo domowników w warunkach pandemii

Od początku pandemii Europol alarmuje o stałym wzroście **liczby i zasięgu cyberprzestępstw i to pomimo wykorzystania starych dobrze znanych metod** (ataki typu ransomware, phishing, dotpay, na bliku itd.).

Coraz częściej celem ataków są nie tylko duże organizacje, **ale także pojedyncze osoby.**

W tej sytuacji **kluczowa jest edukacja nie tylko pracowników – dorosłych, ale także dzieci**, które w warunkach wymuszonej izolacji korzystają z tych samych urządzeń i z tej samej słabo zabezpieczonej sieci domowej.



Przyczyny wzrostu zagrożenia cyberprzestępczością w czasie pandemii

- **Brak wystarczającej liczby urządzeń do pracy zdalnej**

Wszyscy domownicy używają jednego komputera do różnych celów: pracy zawodowej, edukacji szkolnej i rozrywki

- **Niekontrolowany dostęp dzieci do Internetu**

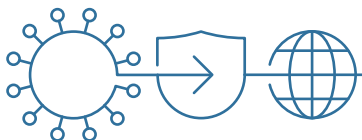
Dzieci nieświadome zagrożeń, cierpiące na nudę i poczucie samotności z powodu izolacji łatwo mogą paść ofiarą cyberataku wymierzonego bezpośrednio w nie lub pośrednio w korzystających z tego samego komputera rodziców

- **Przeciążenie rodziców pracą zdalną**

Również dorośli spędzając znacznie więcej czasu online przestają zachowywać należyłą ostrożność i są bardziej narażeni na próby wykradzenia danych ich organizacji, jak również ich samych i ich rodzin.

- **Niewłaściwie zabezpieczone oprogramowanie do pracy zdalnej**

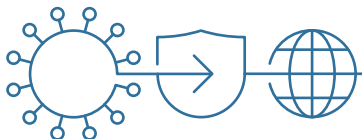
Wybór źle zabezpieczonego komunikatora do pracy zdalnej lub niewłaściwa konfiguracja bezpiecznego programu pozwala cyberprzestępcom zbierać informacje np. przez uzyskanie nieautoryzowanego dostępu do spotkania online



Wzrost aktywności cyberpedofili

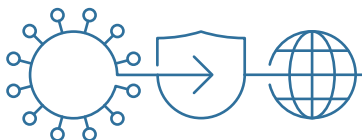
W raportach z kwietnia, czerwca i października 2020 r. Europol zwraca uwagę na znaczny wzrost aktywności cyberpedofili w Internecie. Są to:

- **Próby bezpośredniego kontaktu z dziećmi** w celu wyłudzenia lub wymuszenia przekazania plików z autopornografią.
- **Wzrost aktywności na forach** w darkwebie.
- Przenoszenie komunikacji między cyberpedofilami do coraz **lepiej szyfrowanych komunikatorów**.
- Rosnąca liczba udostępnianych w sieci **plików z pornografią dziecięcą**.
- Popularyzacja **live streamów z pornografią dziecięcą**.
- Zwiększenie ilości **wymiany i handlu plikami w sieciach P2P lub w DarkNecie**.



Inicjatywy edukacyjne związane z cyberbezpieczeństwem

- **Materiały edukacyjne, publikowane w przystępnej formie na stronach internetowych instytucji publicznych** takich jak ENISA, Europol, UODO czy NASK.
- **Organizacja akcji społecznościowych**
Zainicjowane przez Europol kampanie: **#SayNO** - kampania przeciw cyberpedofilii oraz **#TraceanObject** - akcja śledzenia obiektów znajdujących się w tle materiałów z pornografią dziecięcą
- **Gry edukacyjne**
Skierowane zazwyczaj przede wszystkim do młodszych użytkowników sieci. Mają tę przewagę nad innymi działaniami edukacyjnymi, że nie tylko pozwalają zdobyć podstawową wiedzę z zakresu cyberbezpieczeństwa ale również dają możliwość bezpiecznego jej przetestowania w praktyce.



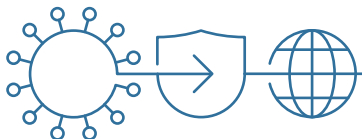
Inicjatywy edukacyjne związane z cyberbezpieczeństwem

76%

polских użytkowników
Internetu to gracze

65%

polских internautów
gra w gry ze swoimi
dziećmi

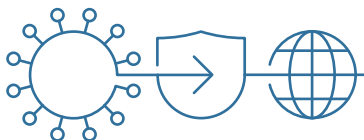


Gry edukacyjne jako skuteczny sposób uczenia

- W odróżnieniu od typowych gier wideo w grach edukacyjnych **rozrywka nie jest celem samym w sobie lecz sposobem na skuteczne przekazanie wiedzy i narzędziem do opanowania nowych umiejętności.**
- Dzięki atrakcyjnej formie przekazu gry edukacyjne wywołują **pozytywne emocje, dają uczucie przyjemności** i w naturalny sposób wspomagają proces uczenia.
- O ogromnym potencjale edukacyjnym gier świadczy popularność procesu **grywalizacji** (z ang. gamification) powszechnie wykorzystywanego w takich obszarach jak edukacja, marketing, sprzedaż, zarządzanie zespołem itp.

Grywalizacja

– wykorzystanie rozwiązań stosowanych w grach w kontekście niezwiązanym z grami mające na celu zwiększanie zaangażowania, zmotywowanie do działania, pobudzanie do nauki i rozwiązywania problemów bądź wywołania pożądanych zachowań.



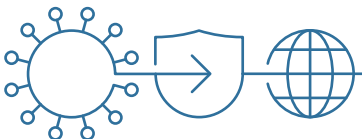
Podstawowe rodzaje komputerowych gier edukacyjnych

Gry treningowe:

ich celem edukacyjnym
jest skłonienie graczy
do wykonywania
określonych czynności,
a przez to trenowanie
związanych z nimi
umiejętności.

Gry informacyjne

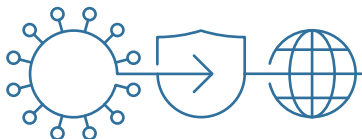
ich celem edukacyjnym
jest **zweryfikowanie**
posiadanej przez gracza
wiedzy i w przypadku jej
braku **uzyskanie**
odpowiednich informacji
w trakcie gry.



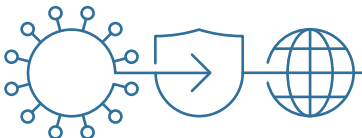
Mechanika gier jako unikalny sposób na efektywne nauczanie

Przykładowe mechanizmy wciągające gracza w świat gry i zwiększające motywację do działania:

- **Wyzwania** – realizacja zadań i osiągnięcie celów
- **Postęp** – określa pozycję gracza na drodze do celu, poziomy trudności
- **Status** – poziomy zaawansowania, odznaki
- **System nagród** – punkty i odznaki za osiągnięcia
- **Rywalizacja** – indywidualna i zespołowa
- **Rankingi** – pozwalają porównać się z innymi
- **Kolekcjonowanie** – zbieranie i handel punktami lub wirtualnymi przedmiotami
- **Niechęć do straty** – lęk przed utratą zdobytych na początku gry wirtualnych dóbr

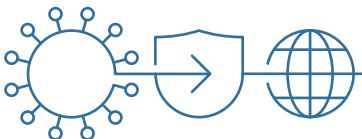


Uczenie się oparte na grach (ang. game-based learning - GBL)



Zalety uczenia się opartego na grach

- Skłaniają do aktywności, prowokują do samodzielnego działania
- Możliwość bezpiecznego eksperymentowania
- Są nie tylko pożyteczne ale również przyjemne
- Są interaktywne, oferują natychmiastową informację zwrotną
- Są stosunkowo łatwe do aktualizowania i adaptacji
- Mogą w naturalny sposób łączyć informacje z różnych dziedzin



Przykłady zastosowań gier edukacyjnych - symulatory

Profesjonalne symulatory szkoleniowe dla lotników, żołnierzy, strażaków itp.

Umożliwiają przygotowanie adeptów do wykonywania skomplikowanych zadań związanych z ich zawodem. Sesje treningowe dają im szansę skonfrontować się z realnym stresem bez ponoszenia prawdziwego ryzyka.



Przykłady zastosowań gier edukacyjnych w biznesie

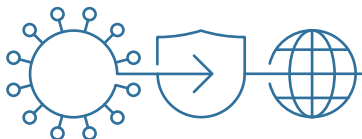
Biznesowe gry edukacyjne

Najczęściej służą do wprowadzenia nowych pracowników w realia funkcjonowania firmy lub zwiększenia kompetencji pracowników bez ponoszenia dodatkowych kosztów szkoleń itp..

IBM's Innov8

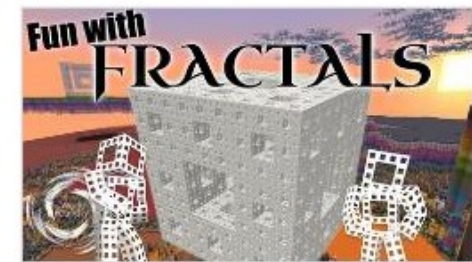


Volkswagen



Przykłady zastosowań gier w edukacji

Minecraft: Education Edition



Przykłady zastosowań gier w edukacji

Rufus w opałach



Cyberbezpieczeństwo w administracji (testowa wersja)



Dziękujemy za uwagę

mgr Konrad Radomiński

k.radominski@uksw.edu.pl

mgr Wawrzyniec Świącicki

w.swiecicki@uksw.edu.pl



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne