„Polityka i Społeczeństwo” 2(22) / 2024
DOI: 10.15584/polispol.2024.2.17

ARTYKUŁY

Krystian Tuczyński*

PHISHING W SZKOLNICTWIE WYŻSZYM: WYZWANIA I STRATEGIE ZAPOBIEGAWCZE W SPOŁECZNOŚCI AKADEMICKIEJ W KONTEKŚCIE ZASTOSOWANIA *E-LEARNINGU*

Streszczenie

Treść artykułu koncentruje się na określeniu wyzwań i strategii zapobiegania zjawiskowi *phishingu* w społeczności akademickiej. Rosnące znaczenie *e-learningu* w edukacji bezprecedensowo stwarza zagrożenia związane z cyberatakami. Autor wskazuje charakterystykę i specyfikę *phishingu* w kontekście szkół wyższych ze szczególnym uwzględnieniem niebezpieczeństw czyhających w kształceniu na odległość. W opracowaniu zaprezentowane zostały środki zaradcze oraz metody minimalizacji zagrożeń internetowych, na które narażeni są nauczyciele akademiccy oraz studenci. Ponadto przedstawiono wnioski podkreślające istotną rolę dalszych działań mających na celu zwiększenie bezpieczeństwa w społeczności akademickiej w kontekście *e-learningu*. Artykuł wieńczy bibliografia, zawierająca źródła wykorzystane w opracowaniu.

Słowa kluczowe: *phishing*, *e-learning*, społeczeństwo, szkolnictwo wyższe

Wstęp

W dynamicznie ewoluującym środowisku szkolnictwa wyższego wykorzystanie platform e-learningowych stało się nieodłącznym elementem postępu akademickiego. Jednakże ten cyfrowy przełom przyniósł ze sobą nowe, złożone wyzwania, z którymi musi zmierzyć się cała społeczność akademicka[1]. Szczególnie w centrum uwagi znajdują się zagrożenia cybernetyczne, a wśród nich tzw. ataki *phishingowe*, które stają się coraz bardziej wyrafinowane i skierowane wobec uczelni wyższych[2].

* Uniwersytet Rzeszowski, e-mail: ktuczynski@ur.edu.pl, ORCID: 0000-0001-8220-2199.

[1] R. Wolert, M. Rawski, *Email phishing detection with BLSTM and word embeddings*. “International Journal of Electronics and Telecommunications”, 2023, nr 69, s. 485–491.

[2] J. Sadowski, *Cybernetyczny wymiar współczesnych zagrożeń*, „Studia nad Bezpieczeństwem”, 2017, nr 2, s. 57–76.

Integracja platform e-learningowych w proces kształcenia akademickiego, choć nieodłączna dla postępu edukacyjnego, stanowi nowy wymiar potencjalnych zagrożeń. Dla hakerów, wykorzystujących coraz bardziej zaawansowane strategie, uczelnie wyższe stanowią bardzo pożądany cel ataku[3]. Społeczność akademicka musi skoncentrować się na rozwinięciu skutecznych strategii obronnych, które zabezpieczą infrastrukturę cyfrową oraz zachowają integralność i zaufanie w środowisku edukacyjnym. Wprowadzenie środków bezpieczeństwa edukacji w zakresie rozpoznawania zagrożeń oraz współpraca pomiędzy instytucjami stają się kluczowe dla utrzymania bezpiecznego i skutecznego środowiska edukacyjnego[4].

Phishing – analiza zjawiska

Phishing, czyli wyszukana forma cyberprzestępczości, stanowi jedno z największych zagrożeń we współczesnej erze cyfrowej[5]. Pochodzenia tego terminu można się doszukać od angielskiego słowa *fishing*, które w wolnym tłumaczeniu oznacza ‘łowienie’. *Phisherzy*, czyli osoby zajmujące się wspomnianą cyberprzestępczością, podobnie jak osoby wędkujące, posługują się różnymi metodami i „wabikami”, aby zdezorientować i oszukać potencjalną ofiarę (w tym przypadku użytkowników internetu)[6].

Ten rodzaj cyberzagrożenia polega na rozsyłaniu fałszywych wiadomości, najczęściej w postaci e-maili, wiadomości SMS lub na innych komunikatorach z zamiarem zdobycia poufnych danych od ofiary. Ataki te są starannie zaplanowane i wykorzystują psychologiczne mechanizmy, aby skłonić ludzi do podejmowania działań bez świadomości konsekwencji. *Phisherzy* niejednokrotnie podszywają się pod instytucje finansowe, bankowe (np. Bank PKO), firmy przewozowe (np. Inpost,

[3] F. Shersad, S. Salam, *Managing risks of e-learning during COVID-19*, “International Journal of Innovation and Research in Educational Sciences”, 2020, nr 7, 2020, s. 348–358.

[4] K. Ciulkin-Sarnocińska, *Phishing – specyficzna forma pozyskiwania danych newralgicznych* [w:] *Współczesne oblicza bezpieczeństwa*, red. E.M. Guzik-Makaruk, W. Pływaczewski, Białystok 2015, s. 113–121.

[5] H. Alghamdi, *Can Phishing Education Enable Users To Recognize Phishing Attacks?*, Dublin 2017.

[6] I. Protasowicki, *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, „Zeszyty Naukowe Wyższej Szkoły Informatyki Zarządzania i Administracji w Warszawie”, 2016, nr 14, s. 35–46.

DHL) znane marki (np. Adidas), tworząc wiadomości, które wydają się autentyczne i potrafią wprowadzić w błąd nawet najbardziej ostrożnych użytkowników.

Jednym z charakterystycznych elementów *phishingu* jest zastosowanie socjotechniki, czyli manipulacji ludzkim zachowaniem. Strach, presja czasu czy chęć szybkiego zarobku są głównymi czynnikami zwiększającymi skuteczność hakerów. W rezultacie użytkownicy stają się podatni na utratę poufnych danych, które mogą być wykorzystane w różnych celach, takich jak kradzież tożsamości, oszustwa finansowe czy ataki na systemy informatyczne.

Wśród najpopularniejszych form *phishingu* wyróżnić można m.in. *spear phishing*, *vishing*, *smishing*, *phishing mail*, *domain spoofing*, *whaling* czy *malvertsing*, lecz niezależnie od rodzaju zawsze celem jest zdobycie poufnych informacji. Pierwszy z wyróżnionych (*spear phishing*) to zaawansowana forma ataku *phishingowego*, skierowana na konkretną osobę lub organizację. Atakujący dokładnie analizują swoje cele, zbierają informacje na ich temat i dostosowują szkodliwe wiadomości do konkretnej sytuacji. Jest to bardzo trudna forma do wykrycia, ponieważ atakujący używają spersonalizowanych i wiarygodnych informacji[7]. *Vishing* to skrót od *voice phishing* i odnosi się do ataków przeprowadzanych za pomocą połączeń telefonicznych. Oszuści niejednokrotnie udają przedstawicieli instytucji finansowych, np. banków lub innych organizacji, w celu przekonania ofiary do ujawnienia poufnych informacji, takich jak numery kont bankowych czy nawet PIN karty kredytowej[8]. *Smishing* powstał z połączenia angielskich słów „SMS" i *phishing*. Ten rodzaj oszustw odnosi się do ataków *phishingowych* przeprowadzanych za pomocą wiadomości tekstowych (SMS) lub multimedialnych (MMS). Podobnie, jak w przypadku *vishingu*, oszuści wysyłają fałszywe informacje, podszywając się pod instytucje finansowe czy firmy[9]. *Phishing email* to rodzaj ataku polegający na wysyłaniu fałszywych wiadomości e-mail, które wydają się pochodzić od zaufanych źródeł. Od dwóch poprzednich różni jedynie medium, za pomocą którego są przesyłane szkodliwe treści[10]. *Domain spoo-*

[7] B. Parmar, *Protecting against spear-phishing*, "Computer Fraud & Security", 2012, nr 1, s. 8–11.

[8] E. Yeboah-Boateng, P. Amanor, *Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices*, "Journal of Emerging Trends in Computing and Information Sciences", 2014, nr 5, s. 297–307.

[9] S. Mishra, D. Soni, *Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis, "*Future Generation Computer Systems", 2020, nr 108, s. 803–815.

[10] A. Almomani [i in.], *A Survey of Phishing Email Filtering Techniques*, "IEEE Communications Surveys & Tutorials", 2013, nr 15, s. 2070–2090.

fing to z kolei typ *phishingu*, w którym atakujący podszywa się pod prawdziwe domeny witryn internetowych, tworząc fałszywe strony, aby uzyskać poufne dane od ofiary[11]. *Whaling* to rodzaj ataku *phishingowego*, który jest ukierunkowany na osoby zajmujące wysokie stanowiska, takie jak kadry dyrektorskie czy kierownicze w firmach. Atakujący starają się wyłudzić od nich istotne informacje lub uzyskać dostęp do strategicznych zasobów firmy[12]. Ostatni z wyróżnionych (*malvertising*) to rodzaj ataku, w którym oszuści umieszczają złośliwe reklamy online, mogące prowadzić do infekcji komputera ofiary lub przekierowywać na strony *phishingowe*[13].

Skutki ataków *phishingowych* mogą być katastrofalne. Spośród najpoważniejszych wyróżnić możemy kradzież tożsamości czy dostęp do kont bankowych. Instytucje padające ofiarą ataków narażają się na utratę zaufania klientów oraz na szkody finansowe. Skuteczne przeciwdziałanie *phishingowi* nie polega jedynie na podniesieniu świadomości poszczególnych użytkowników, ale również na wprowadzeniu efektywnych zabezpieczeń, takich jak filtry *antyphishingowe* czy programy edukacyjne dotyczące bezpieczeństwa online. Zjawisko *phishingu* jest dynamiczne i podlega ciągłym zmianom, co wymusza stałe doskonalenie strategii obronnych, aby skutecznie przeciwdziałać coraz bardziej wyrafinowanym technikom stosowanym przez cyberprzestępców[14].

E-learning akademicki a ryzyko *phishingu*

Wraz z dynamicznym rozwojem technologii *e-learning* stał się nieodłącznym elementem współczesnego szkolnictwa wyższego, oferując studentom elastyczność i dostęp do edukacji bez konieczności fizycznego uczestnictwa w zajęciach[15]. Niezaprzeczalne korzyści wynikające z kształcenia zdalnego generują również nowe wyzwania

[11] A. Herzberg, A. Jbara, *Security and Identification Indicators for Web Browsers against Spoofing and Phishing Attacks*, "ACM Transactions on Internet Technology", 2008, s. 1–45.

[12] V. Bhavsar, A. Kadlak, S. Sharma, *Study on Phishing Attacks*, "International Journal of Computer Applications", 2018, nr 182, s. 27–29.

[13] A.K. Sood, R.J. Enbody, *Malvertising – Exploiting Web Advertising*, "Computer Fraud & Security", 2011, nr 4, s. 11–16.

[14] W. Wróblewski, N. Tuśnio, *Incident Risk Reduction Based on Risk Analysis in the Operational Cyberspace of the Fire Brigade: Cybersecurity Perspective*, "Journal of Management and Security", 2023, nr 50, 2023, s. 445–465.

[15] T. Warchoł, *Kurs e-learningowy: obróbka materiału wideo w programie Pinnacle Studio oparty na teorii kognitywnej procesu uczenia się*, „Edukacja – Technika – Informatyka", 2015, nr 4, s. 169–175.

związane z bezpieczeństwem cyfrowym, a jednym z najpoważniejszych zagrożeń jest *phishing*. Ataki *phishingowe* w procesie kształcenia akademickiego mogą przybrać wiele form. Jedną z nich jest próba podszywania się pod platformę e-learningową (np. Moodle), na której realizowane są zajęcia. W kształceniu zdalnym logowanie do platformy internetowej jest powszechne, w związku z czym ataki *phishingowe* mogą być szczególnie skuteczne. Studenci, zafascynowani ideą zdalnej edukacji, mogą stać się łatwym celem dla cyberprzestępców. Ponadto specyfika *e-learningu* sprawia, że uczestnicy są bardziej skłonni do korzystania z różnych platform, co zwiększa pole manewru dla przestępców[16].

Innym rodzajem ataku jest przesyłanie na adresy mailowe studentów i pracowników akademickich fałszywych e-maili, które sugerują konieczność zalogowania się do swoich kont w celu aktualizacji danych osobowych lub usunięcia zbędnych wiadomości (z powodu braku miejsca w skrzynce mailowej). Linki zawarte w tych wiadomościach kierują jednak do fałszywych stron logowania, gdzie przestępcy przechwytują dane uwierzytelniające.

Kolejnym, równie niebezpiecznym zjawiskiem są wiadomości z ofertami szkoleń online. Atakujący tworzą fałszywe oferty dodatkowych kursów, które wydają się powiązane z instytucją edukacyjną. Studenci oraz nauczyciele akademiccy otrzymujący takie propozycje mogą zostać skłonieni do kliknięcia na szkodliwe linki lub podania swoich danych, myśląc, że uczestniczą w oficjalnym programie szkoleniowym[17].

Wśród ataków *phishingowych* znajdują się również takie, w których użytkownicy informowani są o rzekomych incydentach związanych z przejęciem przez inne osoby ich konta. Osoby otrzymujące takie powiadomienia mogą zareagować bez zastanowienia, klikając w linki lub podając informacje uwierzytelniające w celu rzekomej weryfikacji danych.

E-learning, mimo swoich licznych zalet, niesie ze sobą specyficzne wyzwania związane z bezpieczeństwem cyfrowym. W miarę ewoluowania zagrożeń cybernetycznych konieczne jest ciągłe doskonalenie środków bezpieczeństwa w e-learningu, aby zapewnić bezpieczne i skuteczne środowisko nauki online.

---

[16] M.P. Bach, T. Kamenjarska, B. Žmuk, *Targets of Phishing Attacks: The Bigger Fish to Fry*, "Procedia Computer Science", 2022, nr 204, s. 448–455.

[17] R. Broadhurst [i in.], *Phishing and Cybercrime Risks in a University Student Community*, "International Journal of Cybersecurity Intelligence and Cybercrime", 2018, nr 2, s. 4–23.

Strategie zwalczania *phishingu* w *e-learningu* akademickim

W kontekście bezpieczeństwa *e-learningu* akademickiego istnieje kilka kluczowych i strategicznych elementów, które obejmują szeroko rozumianą kwestię edukacji i świadomości. Działania w tym obszarze powinny być ukierunkowane na organizowanie przez instytucje edukacyjne szkoleń, które w swoim założeniu nie tylko dostarczą specjalistycznej wiedzy, ale także umożliwią świadome rozpoznawanie potencjalnych zagrożeń w sieci. Kampanie edukacyjne, takie jak plakaty czy krótkie filmy, stanowić powinny integralną część tego procesu, wzbogacając wiedzę nauczycieli akademickich i studentów o zasady bezpieczeństwa online[18].

Kolejnym kluczowym aspektem w kontekście ochrony przed zagrożeniami cybernetycznymi w *e-learningu* jest przeprowadzanie przez centra informatyzacji symulacji ataków. Regularne testy w postaci przesyłania testowych wiadomości przypominających w swojej formie ataki *phishingowe* są istotne dla oceny skuteczności działań edukacyjnych. Dzięki nim możliwe jest identyfikowanie obszarów wymagających poprawy oraz doskonalenie umiejętności rozpoznawania i unikania potencjalnych zagrożeń[19].

Ważnym środkiem zapobiegawczym jest także stosowanie tzw. filtrów *antyphishingowych*. Instytucje edukacyjne powinny ich używać w systemach poczty e-mail. Oparte na zaawansowanych algorytmach analizy treści mają kluczowe znaczenie dla efektywnej identyfikacji i blokowania podejrzanych wiadomości, zabezpieczając tym samym uczestników przed atakami *phishingowymi*[20].

Ważnym aspektem jest również systematyczny monitoring aktywności sieciowej. Ciągła analiza ruchu w sieci umożliwia szybkie wykrywanie wszelkich nieprawidłowości czy podejrzanych zachowań, co pozwala na skuteczną reakcję na potencjalne zagrożenia w czasie rzeczywistym, a także zabezpiecza infrastrukturę e-learningową.

Ostatnim, niemniej istotnym elementem jest regularna aktualizacja oprogramowania, zarówno na poziomie uczestników *e-learningu*, jak

[18] S. Chaudhary [i in.], *Time Up for Phishing with Effective Anti-Phishing Research Strategies*, "International Journal of Human Capital and Information Technology Professionals", 2015, nr 6, s. 49–64.

[19] Z. Wardaszka, *Narzędzie do ciągłej edukacji użytkowników internetu o atakach typu e-mail phishing za pomocą symulacji*, Praca inżynierska obroniona w Politechnice Warszawskiej, Wydział Elektroniki i Technik Informacyjnych, 2023.

[20] A. Stępień, *Bezpieczeństwo Polski w cyberprzestrzeni*, „Przedsiębiorczość i Zarządzanie", 2013, nr 5, s. 231–244.

i infrastruktury edukacyjnej. Wspomniane działanie chroni przed znajdowaniem niedoskonałości zabezpieczeń systemów, co stanowi potencjalne zagrożenie ze strony cyberprzestępców.

Wspólne działanie na rzecz bezpieczeństwa społeczności akademickiej

Kompleksowe działanie na rzecz bezpieczeństwa społeczności akademickiej w kontekście *phishingu* obejmuje szereg kluczowych aspektów. Pierwszym z nich jest skuteczna wymiana informacji pomiędzy wszystkimi użytkownikami lokalnej sieci. Zabieg ten umożliwia błyskawiczną komunikację na temat nowych zagrożeń i gwałtowną reakcję w opracowywaniu strategii przeciwdziałania wspomnianym zjawiskom. Poprzez dzielenie się doświadczeniami z wykrytych ataków uczelnie mogą tworzyć plan działania umożliwiający skoordynowaną reakcję na zagrożenia *phishingowe*.

Kolejnym aspektem jest utworzenie tzw. centrów bezpieczeństwa cybernetycznego. Wspomniane jednostki umożliwiać mogą sprawne i kompleksowe działania w zakresie monitorowania, analizy i reagowania na zaawansowane ataki *phishingowe*. Współpraca na poziomie centrów bezpieczeństwa cybernetycznego przyczyniłaby się do zwiększenia bezpieczeństwa społeczności akademickiej oraz skutecznego przeciwdziałania zagrożeniom internetowym[21].

Tworzenie standardów bezpieczeństwa jest kolejnym kluczowym elementem wspólnego działania. Współpraca pozwala na rozwinięcie standardów bezpieczeństwa, które obowiązują na szerszym obszarze społeczności akademickiej. Opracowanie jednolitych wytycznych dotyczących bezpieczeństwa IT i korzystania z zasobów online ułatwia wdrożenie skutecznych praktyk przeciwdziałającym zagrożeniom internetowym[22].

Wsparcie od instytucji rządowych stanowiłby istotny aspekt wspólnego wysiłku w zwalczaniu *phishingu*. Współpraca społeczności akademickiej z rządem i sektorem prywatnym obejmować może dostęp do najnowszych narzędzi i rozwiązań bezpieczeństwa oraz korzystanie z ekspertyz w dziedzinie cyberbezpieczeństwa. Działa to na rzecz stwo-

[21] P. Mickiewicz, *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego", 2017, nr 11, s. 65–80.

[22] K. Liderman, *Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki", 2009, nr 26, s. 29–43.

rzenia kompleksowego systemu wsparcia dla społeczności akademickiej w zakresie bezpieczeństwa cyfrowego.

Skoordynowane i wspólne działania społeczności akademickiej w wymienionych obszarach są niezbędne do skutecznego przeciwdziałania zagrożeniom *phishingowym*. Współpraca ta powinna obejmować nie tylko reakcję na incydenty, lecz także aktywne inicjatywy prewencyjne i edukacyjne, tworząc kompleksowe podejście do bezpieczeństwa cyfrowego.

Zakończenie

Phishing, będący bardzo zaawansowanym rodzajem cyberprzestępczości, stanowi poważne zagrożenie dla wszystkich użytkowników internetu. Celem ich ataku są zarówno instytucje finansowe i rządowe, jak również cała wirtualna społeczność. Instytucje edukacyjne prowadzące kształcenie zdalne (*e-learning*) również narażone są na ryzyko związane z *phishingiem*. Przeciwdziałanie temu zjawisku stanowić może odpowiednia edukacja uczestników, stosowanie filtrów *antyphishingowych*, monitorowanie aktywności sieciowej i regularne aktualizacje oprogramowania. Kluczowe znaczenie ma współpraca między instytucjami edukacyjnymi, rządem i sektorem prywatnym. Również wsparcie społeczności akademickiej jest niezbędne dla skutecznej walki z *phishingiem*. Walka z *phishingiem* w *e-learningu* wymaga wielowymiarowego podejścia, łączącego zarówno edukację, technologiczne środki ochronne, jak również współpracę między różnymi instytucjami. Współpraca społeczności akademickiej stanowi klucz dla skutecznego przeciwdziałania temu zagrożeniu.

Bibliografia

Alghamdi H., *Can Phishing Education Enable Users To Recognize Phishing Attacks?*, Dublin 2017, doi:10.21427/D7DK8T.

Almomani A. [i in.], *A Survey of Phishing Email Filtering Techniques*, "IEEE Communications Surveys & Tutorials", 2013, nr 15.

Bach M.P., Kamenjarska T., Žmuk B., *Targets of Phishing Attacks: The Bigger Fish to Fry*, "Procedia Computer Science", 2022, nr 204.

Bhavsar V., Kadlak A., Sharma S., *Study on Phishing Attacks*, "International Journal of Computer Applications", 2018, nr 182.

Broadhurst R. [i in.], *Phishing and Cybercrime Risks in a University Student Community*, "International Journal of Cybersecurity Intelligence and Cybercrime", 2018, nr 2.

Chaudhary S. [i in.], *Time Up for Phishing with Effective Anti-Phishing Research Strategies*, "International Journal of Human Capital and Information Technology Professionals", 2015, nr 6.

Ciulkin-Sarnocińska K., *Phishing – specyficzna forma pozyskiwania danych newralgicznych* [w:] *Współczesne oblicza bezpieczeństwa*, red. E.M. Guzik-Makaruk, W. Pływaczewski, Białystok 2015.

Herzberg A., Jbara A., *Security and Identification Indicators for Web Browsers against Spoofing and Phishing Attacks*, "ACM Transactions on Internet Technology", 2008, doi: 10.1145/1391949.1391950.

Liderman K., *Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki", 2009, nr 26.

Mickiewicz P., *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego", 2017, nr 11.

Mishra S., Soni D., *Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis, "*Future Generation Computer Systems", 2020, nr 108.

Parmar B., *Protecting against spear-phishing*, "Computer Fraud & Security", 2012, nr 1, doi: 10.1016/S1361-3723(12)70007-6.

Protasowicki I., *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, „Zeszyty Naukowe Wyższej Szkoły Informatyki Zarządzania i Administracji w Warszawie", 2016, nr 14.

Sadowski J., *Cybernetyczny wymiar współczesnych zagrożeń*, „Studia nad Bezpieczeństwem", 2017, nr 2.

Shersad F., Salam S., *Managing risks of e-learning during COVID-19*, "International Journal of Innovation and Research in Educational Sciences", 2020, nr 7.

Sood A.K., Enbody R.J., *Malvertising – Exploiting Web Advertising*, "Computer Fraud & Security", 2011, nr 4.

Stępień A., *Bezpieczeństwo Polski w cyberprzestrzeni*, „Przedsiębiorczość i Zarządzanie", 2013, nr 5.

Warchoł T., *Kurs e-learningowy: obróbka materiału wideo w programie Pinnacle Studio oparty na teorii kognitywnej procesu uczenia się*, „Edukacja – Technika – Informatyka", 2015, nr 4.

Wardaszka Z., *Narzędzie do ciągłej edukacji użytkowników internetu o atakach typu e-mail phishing za pomocą symulacji*, Praca inżynierska obroniona w Politechnice Warszawskiej, Wydział Elektroniki i Technik Informacyjnych, 2023.

Wolert R., Rawski M., *Email phishing detection with BLSTM and word embeddings*. "International Journal Of Electronics And Telecommunications", 2023, nr 69, doi:10.24425/ijet.2023.146496.

Wróblewski W., Tuśnio N., *Incident Risk Reduction Based on Risk Analysis in the Operational Cyberspace of the Fire Brigade: Cybersecurity Perspective*, "Journal of Management and Security", 2023, nr 50, doi:10.13166/jms/161536.

Yeboah-Boateng E., Amanor P., *Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices*, "Journal of Emerging Trends in Computing and Information Sciences", 2014, nr 5.

Phishing in Higher Education: Challenges and Preventive Strategies in the Academic Community in the Context of E-learning

Abstract

The article focuses on identifying challenges and preventive strategies related to the phenomenon of phishing within the academic community. The growing significance of e-learning in education has unprecedentedly introduced cyber threats, particularly those associated with phishing attacks. The author outlines the characteristics and specifics of phishing in the context of higher education, with a special emphasis on the dangers posed by e-learning. The paper presents remedial measures and methods to minimize online threats for academic teachers and students. Furthermore, the article highlights conclusions underscoring the significant role of further research and actions aimed at strengthening security within the academic community in the context of e-learning. The conclusion includes a bibliography, showcasing the sources utilized in the development of the article.

Keywords: phishing, e-learning, society, higher education