

NASK

(Cyber)bezpieczne święta, czyli jak się nie dać nabić w... bombkę

Katarzyna Gańko, Zespół Programów Edukacyjno-
-Informacyjnych, NASK

nask.pl



PHISHING I SOCJOTECHNIKA

Najłatwiejszą metodą kradzieży informacji czy zainfekowania urządzenia złośliwym oprogramowaniem jest nakłonienie nas do udostępnienia swoich danych, kliknięcia w niebezpieczny link czy ściągnięcia np. niebezpiecznej aplikacji.

To **socjotechnika**, czyli różne sposoby wywierania wpływu, np. przy użyciu perswazji, manipulacji, zastraszania, szantażu.

NASK



PHISHING I SOCJOTECHNIKA

- Zwracajcie szczególną uwagę na SMS-y z prośbą o dopłatę do paczki, a także podejrzane e-maile, które zawierają błędy językowe i manipulujące komunikaty (np. „podaj dane w ciągu 24 godzin”) oraz są skierowane do ogólnego odbiorcy.
- Jeśli taka wiadomość trafi do Waszej skrzynki, zachowajcie ostrożność: **nie klikajcie w żadne linki i nie dokonujcie płatności**. Zwracajcie szczególną uwagę na rozszerzenie załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości.

NASK



PHISHING I SOCJOTECHNIKA

- Uważajcie też na wiadomości, które rzekomo pochodzą od Waszych znajomych, jednak ani ton wypowiedzi, ani używane zwroty nie pasują do nadawców. Upewnijcie się, czy to faktycznie znajomy próbował się z Wami kontaktować – choćby dzwoniąc do niego.
- Wszystkie podejrzane treści zgłaszajcie do CERT Polska za pośrednictwem formularza na stronie cert.pl. Podejrzane SMS-y możecie przesyłać na numer **8080**.

NASK





2

BEZPIECZEŃSTWO ROZMÓW ONLINE

- W święta „wszyscy wszystkim ślą życzenia” i na szczęście nie musimy już polegać tylko na papierowych kartkach. Dzięki komunikatorom internetowym i oprogramowaniu umożliwiającemu nawiązywanie rozmów wideo możemy być bliżej z przyjaciółmi i rodziną, nawet jeśli w rzeczywistości dzielą nas tysiące kilometrów.
- Aby te kontakty były bezpieczne, musicie pamiętać przede wszystkim o bieżącym **aktualizowaniu** komunikatorów zainstalowanych na komputerach, tabletach czy smartfonach.



2

BEZPIECZEŃSTWO ROZMÓW ONLINE

- Nie bez znaczenia jest także zasada ograniczonego zaufania: nie klikajcie bezrefleksyjnie we wszystkie linki, które dostaniecie w wiadomościach, uważajcie też na podejrzane załączniki i prośby o dołączenie do grona znajomych wysyłane przez obce osoby.
- W rozmowie przy użyciu komunikatorów nigdy **nie podawajcie poufnych informacji** – danych osobowych, loginów i haseł, kodów BLIK czy numerów kont bankowych.



2

BEZPIECZEŃSTWO ROZMÓW ONLINE

- Prowadząc wideorozmowę, nie możecie zapominać o ochronie swojej prywatności. Zastanawiajcie obiektyw kamery, gdy jej nie używacie, a także sprawdzajcie... co macie za plecami. Usuńcie z tła wszystko, co może zawierać osobiste informacje.
- Korzystajcie tylko z aplikacji pochodzących z oficjalnych źródeł.

SHARENTING

- Lubimy uwieczniać wyjątkowe, świąteczne chwile na zdjęciach. Zanim jednak zdecydujecie się podzielić nimi w sieci, dwa razy się zastanówcie. Czy zdjęcie lub filmik przedstawiający Wasze dziecko go nie ośmiesza?
- Sharenting to nieroztropne dokumentowanie życia dziecka w internecie. Klikając „Udostępnij”, musicie mieć świadomość, że pozornie niewinna fotka lub śmieszny filmik mogą obieć internet, trafić w niepowołane ręce lub sprawić, że dziecko stanie się w przyszłości obiektem hejtu, a nawet ofiarą cyberprzemocy.

NASK



3

SHARENTING

W tym przypadku mniej znaczy więcej. Sprawdzajcie **ustawienia prywatności** – tak, by udostępniać materiały tylko znajomym, zrezygnujcie z publikowania zdjęć dzieci rozebranych do kąpieli lub umorusanych jedzeniem i **zawsze pytajcie o zgodę** przed dodaniem zdjęcia czy filmiku.

NASK



3



ZBIÓRKI CHARYTATYWNE ONLINE

- W święta chętniej niż zwykle dzielimy się z potrzebującymi tym, co mamy. Niestety – oszuści potrafią to wykorzystać.
- Przestępcy grają na naszych emocjach i bez mrugnięcia okiem wykorzystują różne metody – wyszukują w internecie zdjęcia chorych dzieci i zwierząt, podrabiają dokumentację medyczną, w swoje zbiórki angażują celebrytów. Wszystko po to, by wyłudzić od nas pieniądze.



ZBIÓRKI CHARYTATYWNE ONLINE

Korzystajcie ze sprawdzonych platform zbiórkowych i **weryfikujcie organizatorów**. Koniecznie zajrzyjcie też na stronę zbiorki.gov.pl, gdzie prowadzony jest rejestr zbiórek publicznych organizowanych na terenie kraju. Sprawdźcie regulamin, daty zbiórki, a jeśli wspieracie akcję stacjonarnie – upewnijcie się, że wolontariusz ma prawidłowy identyfikator zawierający imię i nazwisko, nazwę zbiórki, jej cel i numer, a także informacje o organizatorze.

Jeśli macie podejrzenia co do legalności jakiegś zbiórki pieniędzy, zgłóście tę sprawę na policję.

GRA KOMPUTEROWA NA PREZENT

Gry komputerowe mają wiele zalet: pomagają zdobywać praktyczne umiejętności, rozwijać zainteresowania, wzmacniać kompetencje społeczne, a także budować wieloletnie przyjaźnie. Zanim jednak zapakujecie grę w świąteczny papier i położycie ją pod choinkę, wybierzcie mądrze!

NASK



5

GRA KOMPUTEROWA NA PREZENT

Kierujcie się oznaczeniami PEGI – znajdziecie je na pudełku. Podawane są one na dwa sposoby: w formie pięciu oznaczeń wiekowych (PEGI 3, PEGI 7, PEGI 12, PEGI 16 i PEGI 18) oraz ośmiu deskryptorów treści, czyli oznaczeń zawartości gry (Violence – sceny przemocy, Bad language – wulgaryzmy, Fear – obrazy lub dźwięki, które mogą przestraszyć dziecko, Gambling – elementy hazardowe, Sex – treści o charakterze seksualnym, Drugs – narkotyki i inne używki, Discrimination – stereotypy, In-game purchases – mikropłatności).

NASK



5

GRA KOMPUTEROWA NA PREZENT

Znajomość oznaczeń w systemie PEGI może pomóc w doborze gry odpowiedniej do wieku i możliwości poznawczych dziecka. To jednak nie wszystko! Aby czas spędzony z grą był bezpieczny, potrzebna jest także **rozmowa z młodym graczem i wspólne ustalenie zasad**.

NASK





6

FAŁSZYWE SKLEPY INTERNETOWE

Polubiliśmy sklepy internetowe i często – zwłaszcza przed świętami – decydujemy się na zakupy online. Wygoda, oszczędność czasu, możliwość porównania wielu ofert, korzystne ceny...

Niech nie zwiodą Was „wyjątkowe oferty dostępne tylko dziś”, „megarabaty” i przeceny na cały asortyment!



6

FAŁSZYWE SKLEPY INTERNETOWE

Zanim wrzucicie coś do internetowego koszyka, poszukajcie podstawowych informacji na stronie sklepu: danych kontaktowych (w tym formularza), numeru NIP i numeru wpisu do Krajowego Rejestru Sądowego (KRS), a także regulaminu, informacji o sposobach dostawy, formach płatności czy warunkach zwrotu towaru.



6

FAŁSZYWE SKLEPY INTERNETOWE

- Przed dokonaniem zakupu zapoznajcie się też z opiniami na temat sklepu i sprzedawcy. Waszą czujność powinny wzbudzić wyłącznie pozytywne oceny dodane w podobnym okresie.
- Gdy podejmiecie już decyzję i przejdziecie do strony płatności, sprawdźcie wszystko dwa razy. Jeśli zauważyliście literówki (np. w adresie) lub cokolwiek wzbudzi Wasze podejrzenia – czym prędzej zrezygnujcie z transakcji.

CYFROWE PREZENTY

Jeśli pod choinką znajdzie się tablet, laptop czy smartfon, zadbajcie o ich bezpieczne skonfigurowanie. Zainstalujcie program antywirusowy, wykonajcie aktualizacje systemu i ustawcie podstawowe zabezpieczenia.

NASK



CYFROWE PREZENTY

Pamiętajcie też o zabezpieczeniu urządzeń internetu rzeczy, podłączanych do domowej sieci W-Fi. Wybierajcie sprzęt renomowanych producentów, zmieniajcie domyślne dane logowania, regularnie aktualizujcie oprogramowanie. Jeśli nie ma takiej potrzeby, nie udostępniajcie urządzeniom danych na swój temat.

NASK





8

HIGIENA CYFROWA

- W święta warto zadać o higienę cyfrową – całą rodziną! Ustalcie zasady używania telefonów i internetu i wspólnie ich przestrzegajcie.
- Na początek określcie limit czasu, jaki można spędzać przed ekranem urządzenia. Wyznaczcie też w domu jedno miejsce na odkładanie i ładowanie sprzętów. Umówcie się, że nie będziecie korzystać z ekranów zaraz po przebudzeniu i spróbujecie wyzbyć się nawyku noszenia telefonu zawsze przy sobie.



8

HIGIENA CYFROWA

- Postarajcie się odkładać urządzenia na czas posiłków, spotkań z bliskimi oraz co najmniej godzinę przed snem. Zaoszczędzony czas możecie spędzić całą rodziną, np. na jakiejś aktywności na świeżym powietrzu lub zabawie offline.
- Może podejmiecie **rodzinny offline challenge**? Zasada tego wyzwania jest jedna: odłączamy się od sieci na 48 godzin.. Przyjrzyście się swoim cyfrowym nawykom i sprawdźcie, jak bardzo na co dzień pochłania Was wirtualna rzeczywistość.

DEZINFORMACJA

W gąszczu treści świątecznych i okołoswiątecznych łatwo trafić na zmanipulowane nagrania, w tym deepfake'i. Zachowajcie ostrożność, zwłaszcza wobec sensacyjnych lub emocjonalnych treści – **nie wszystko, co pojawia się w internecie, jest prawdą!**

NASK





10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Silne hasła.** To podstawa ochrony kont i urządzeń. Podczas tworzenia hasła unikajcie oczywistych kombinacji typu „123456” czy „password”. Stosujcie długie (minimum 14 znaków) i unikatowe zabezpieczenia – różne do wielu kont – oraz korzystajcie z menedżerów haseł, które pomagają je przechowywać i zarządzać nimi.



10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Uwierzytelnianie dwuskładnikowe (2FA).** Stanowi dodatkową warstwę zabezpieczeń – poza silnym hasłem. Dzięki 2FA, nawet gdy ktoś pozna Wasze hasło, nie zaloguje się bez potwierdzenia, np. kodem SMS lub wygenerowanym przez aplikację. Włączajcie uwierzytelnianie dwuskładnikowe wszędzie tam, gdzie to możliwe.



PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Aktualizacje systemu i oprogramowania.** To prawdziwa tarcza przed zagrożeniami i kolejny prosty, a zarazem skuteczny sposób ochrony. Dbajcie o regularne aktualizacje systemu operacyjnego, aplikacji i antywirusów. Producenci na bieżąco usuwają wykryte luki i poprawiają zabezpieczenia – ignorowanie update'ów oznacza otwarcie furtki przestępcom.



PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Uwaga na linki i załączniki.** Nie klikajcie w linki i nie pobierajcie załączników przesyłanych od nieznanych nadawców w wiadomościach e-mail, SMS czy w komunikatorach – szczególnie jeśli ktoś każe Wam działać pod presją czasu, bez zastanowienia. Zwracajcie też uwagę na rozszerzenia plików.



10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Fałszywe strony.** Zanim gdziekolwiek wpiszeć swoje dane uwierzytelniające (login i hasło), upewnijcie się, że strona, na której się znajdujecie, jest prawdziwa. Przede wszystkim zwróćcie uwagę na jej adres. Nawet drobna różnica – literówka, dodatkowy znak czy inna końcówka domeny – może oznaczać, że jesteście na fałszywej stronie, która służy do wyłudzenia danych lub pieniędzy. Zielona kłódka nie jest już gwarantem bezpieczeństwa!



10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Świadome korzystanie z mediów społecznościowych.** Bądźcie ostrożni z udostępnianiem osobistych informacji, takich jak numer telefonu czy adres. Stosujcie ustawienia prywatności w social mediach, tak aby Wasze dane nie były publicznie dostępne. Każda informacja może być wykorzystana przez oszustów!



10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

- **Niebezpieczne znajomości w sieci.** Zachowajcie czujność wobec osób poznanych online, które szybko proszą o prywatne dane lub pieniądze. Nie ufajcie nieznajomym, zwłaszcza jeśli ich zachowanie budzi Wasze podejrzenia. W razie wątpliwości korzystajcie z funkcji blokowania i zgłaszania użytkowników na portalach społecznościowych oraz w komunikatorach. Pamiętajcie – Wasze bezpieczeństwo i komfort w relacjach online są najważniejsze!



10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

Reagujcie! Jeśli podejrzewacie próbę oszustwa, możecie zgłosić ją w prosty sposób: wystarczy wypełnić formularz internetowy na stronie cert.pl lub przesłać otrzymaną wiadomość SMS na numer **8080**, korzystając z funkcji „przekaż” lub „udostępnij”. Nie musicie mieć pewności, że to faktycznie oszustwo – zgłoszenie zostanie zweryfikowane przez specjalistów zajmujących się cyberbezpieczeństwem.



10

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

Dlaczego warto? Wasze zgłoszenia mają realny wpływ na bezpieczeństwo w sieci! Dzięki nim niebezpieczne strony trafiają na listę ostrzeżeń, co uniemożliwia dostęp do nich i chroni innych użytkowników przed utratą danych czy pieniędzy. Z kolei podejrzane SMS-y pomagają tworzyć wzorce niebezpiecznych wiadomości, które operatorzy mogą skutecznie blokować, zanim dotrą do kolejnych odbiorców.

higiena cyfrowa

220 nowych
i odświeżonych definicji

profilaktyka

cyberbezpieczeństwo



ABC cyberbezpieczeństwa 2.0

reagowanie

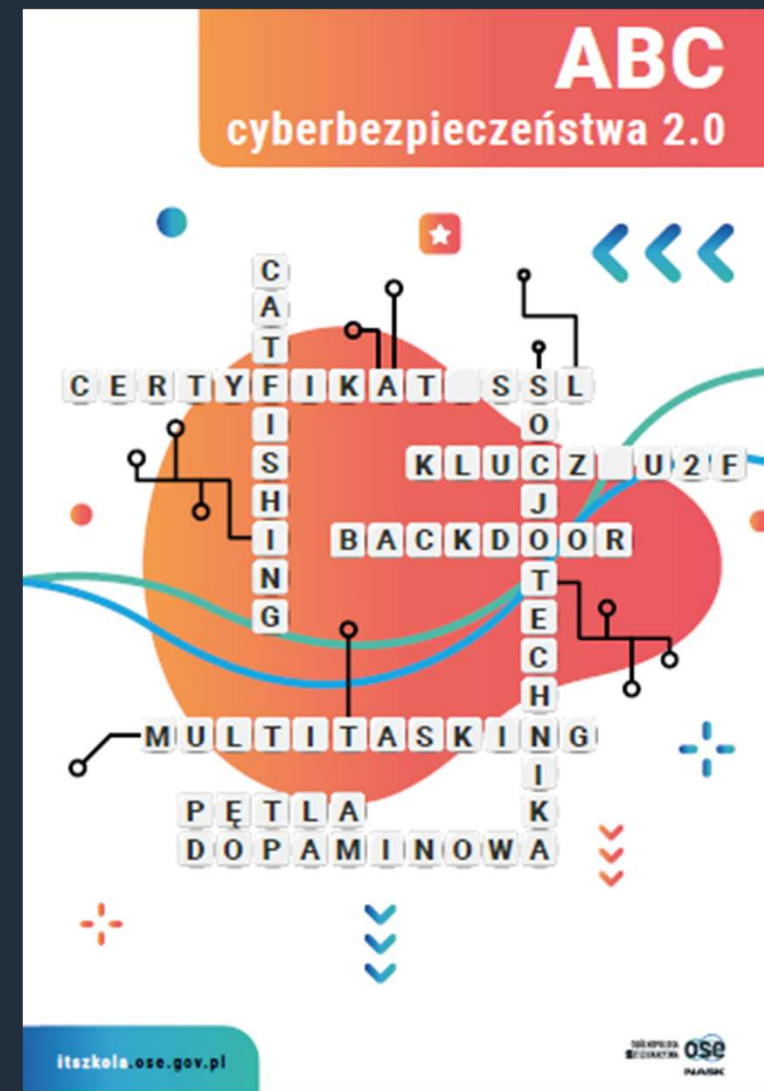
Aktualna wiedza

wsparcie

MINIKONKURS

1. Pobierz „ABC cyberbezpieczeństwa 2.0”:
https://it-szkola.edu.pl/publikacje,plik_117
2. Zastanów się, jak wykorzystać tę publikację w pracy z uczniami.
3. Przygotuj odpowiedź w formie krótkiego opisu ćwiczenia (maks. 1000 znaków ze spacjami).
4. Prześlij odpowiedź na adres osehero@nask.pl do 12.12.2025 do 23:59, wpisując w tytule wiadomości **ABC 2.0 – konkurs – 9.12.**

Nagrodzimy 5 najlepszych zgłoszeń!



Dziękuję za uwagę, życzę
spokojnych, radosnych,
(cyber)bezpiecznych świąt!

katarzyna.ganko@nask.pl