ZAGROŻENIA W INTERNECIE

KLASA VI


ZAKUPY INTERNETOWE

CZY CZĘSTO ROBISZ ZAKUPY W INTERNECIE? JEŚLI TAK, TO SŁUCHAJ UWAŻNIE!

Z PEWNOŚCIĄ WIELU Z NAS ROBI ZAKUPY ONLINE. JEST TO WYGODNE I SZYBKIE, ALE NIESIE TO ZE SOBĄ RÓŻNE ZAGROŻENIA.

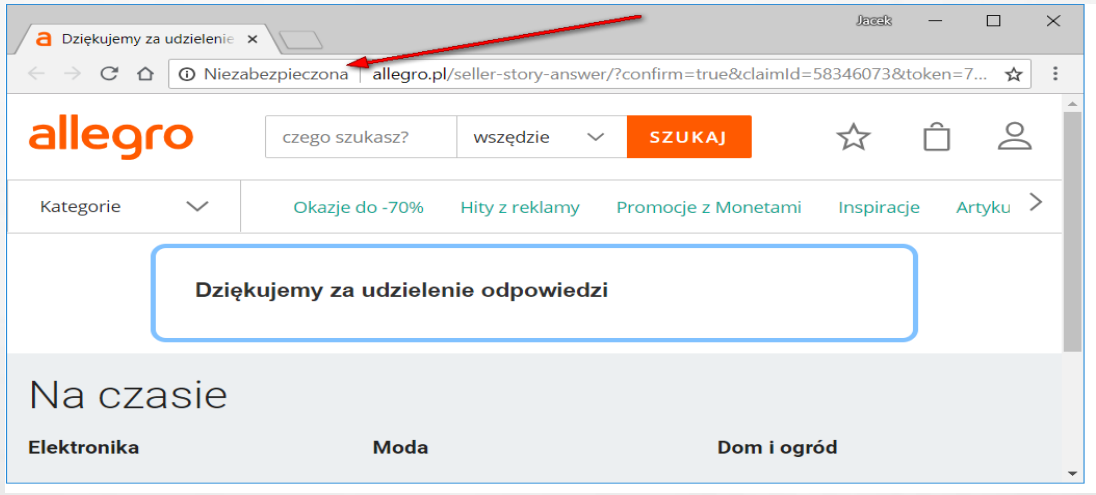
JAKIE ZAGROŻENIA WIĄŻĄ SIĘ Z ZAKUPAMI W SIECI?

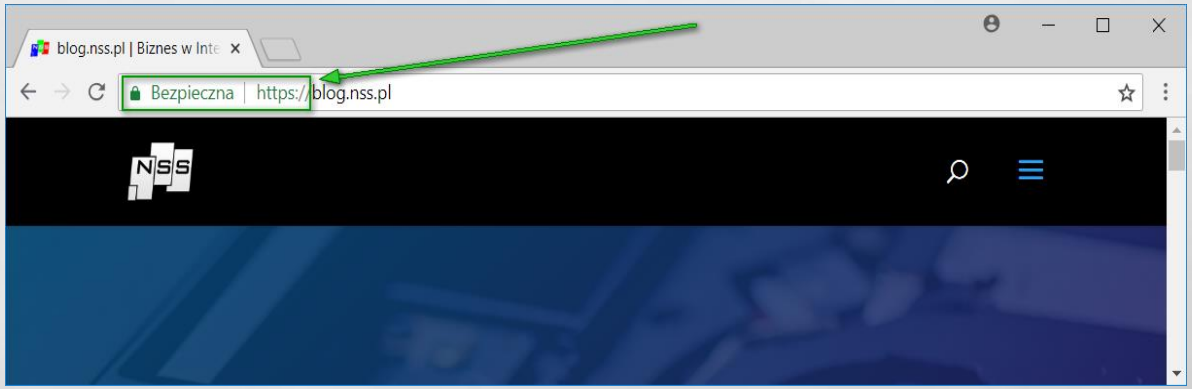
- STRONA MOŻE MIEĆ WIRUSY, GDY NIE JEST ZWERYFIKOWANA
- CZĘSTO PRODUKTY SĄ PODEJRZANIE TANIE. WIELE OSÓB MYŚLI, ŻE TO ŚWIETNA OKAZJA, LECZ KLIENT MOŻE NIGDY NIE DOSTAĆ PRODUKTU, ANI ZWROTU PIENIĘDZY
- NA STRONACH INTERNETOWYCH MOGĄ BYĆ **FAŁSZYWE LINKI**, KTÓRE PRZEKIEROWUJĄ KLIENTA NA INNĄ STRONĘ. PODANIE SWOICH DANYCH UMOŻLIWI CYBERPRZESTĘPCOM ZHAKOWANIE ICH LUB ZAINSTALOWANIE **SPYWARE** – OPROGRAMOWANIA SZPIEGUJĄCEGO. W TEN SPOSÓB MOGĄ NP. DOKONAĆ KRADZIEŻY Z RACHUNKU BANKOWEGO

JAK BEZPIECZNIE KUPOWAĆ ONLINE?

- WYBIERAJ SKLEPY Z CERTYFIKATAMI I ZWERYFIKOWANE
- JEŚLI JEST TAKA MOŻLIWOŚĆ, ZAINSTALUJ PROGRAM WYKRYWAJĄCY WIRUSY
- WYBIERAJ BEZPIECZNE FORMY PŁATNOŚCI
- SZUKAJ **SYMBOLU KŁÓDKI** PRZY STRONIE, TO OZNACZA, ŻE JEST BEZPIECZNA
- SPRAWDŹ, CZY W PRZEGLĄDARCE NA POCZĄTKU ADRESU WITRYNY WIDNIEJE "**HTTPS**" ZAMIAST "HTTP"

PO CZYM POZNAĆ, ŻE STRONA JEST BEZPIECZNA?





PO CZYM POZNAĆ, ŻE STRONA JEST BEZPIECZNA?

- SPRAWDŹ **DANE SPRZEDAWCY**: NIP, REGON, ADRES SIEDZIBY, PEŁNA NAZWA…
- W PASKU ADRESU INTERNETOWEGO SPRAWDŹ, CZY SKLEP MA ZAINSTALOWANY CERTYFIKAT SSL (NAJCZĘŚCIEJ WYŚWIETLA SIĘ **ZIELONA KŁÓDKA**)
- SPRAWDŹ CZY SKLEP UŻYWA ZAUFANYCH BRAMEK PŁATNOŚCI
- SPRAWDŹ OPINIE NA TEMAT SKLEPU (WIZYTÓWKI GOOGLE, PORTALE SPOŁECZNOŚCIOWE, SERWISY AGREGUJĄCE)

JAK BEZPIECZNIE PŁACIĆ W INTERNECIE?

- UPEWNIJ SIĘ, ŻE PRZEKIEROWANIE JEST NA STRONĘ BANKU, JEŚLI PŁACISZ E-PRZELEWEM.
- DOKONUJ PŁATNOŚCI TYLKO NA ZAUFANYCH URZĄDZENIACH Z OPROGRAMOWANIEM ANTYWIRUSOWYM.
- WYBIERAJ BEZPIECZNE METODY PŁATNOŚCI, TAKIE JAK PŁATNOŚĆ E-PRZELEWEM, TRADYCYJNY PRZELEW BANKOWY, BLIK, KARTA KREDYTOWA LUB DEBETOWA, PORTFEL WIRTUALNY LUB PAYSAFECARD

UWAŻAJ NA ZAGROŻENIA!

- NIE KAŻDY SKLEP DZIAŁAJĄCY W **INTERNECIE** JEST PRAWDZIWY – WIELE NIELEGALNYCH WITRYN KORZYSTA NA NIEUWADZE KUPUJĄCYCH, PODSZYWAJĄC SIĘ NP. POD ZNANE SIECI I MARKI
- KORZYSTANIE Z PUBLICZNEJ SIECI WI-FI PODCZAS ZAKUPÓW PODNOSI RYZYKO UTRATY POUFNYCH DANYCH – PŁATNOŚCI NAJLEPIEJ DOKONYWAĆ W DOMU, KORZYSTAJĄC Z ZABEZPIECZONEJ SIECI
- KORZYSTANIE Z NIEZABEZPIECZONYCH STRON MOŻE SKUTKOWAĆ UTRATĄ DANYCH
- OPINIE KLIENTÓW NIE ZAWSZE SĄ WIARYGODNE – WIELU OSZUSTÓW KORZYSTA ZE WSPARCIA DODATKOWYCH OSÓB ZAMIESZCZAJĄCYCH OPINIE NA TEMAT SKLEPU

JAK SIĘ BRONIĆ?

- UWAŻAJ NA LINKI I WIADOMOŚCI E-MAIL OD NIEZNANYCH LUB PODEJRZANYCH NADAWCÓW.
- USTAW SILNE HASŁA I AKTUALIZUJ OPROGRAMOWANIE SYSTEMOWE ORAZ PROGRAMY ANTYWIRUSOWE.
- PAMIĘTAJ, ABY NIGDY NIE UDOSTĘPNIAĆ SWOICH DANYCH OSOBOWYCH LUB INFORMACJI FINANSOWYCH ONLINE.

PRZESTRZEGAJ NASTĘPUJĄCYCH ZASAD

- NIE PODAWAJ SWOICH PRAWDZIWYCH DANYCH OSOBOWYCH, TAKICH JAK IMIĘ, NAZWISKO, ADRES CZY NUMER TELEFONU.
- WYMYŚL SOBIE JAKIŚ **NICK** (NAZWĘ NIE ZWIĄZANĄ Z TWOIMI DANYMI PERSONALNYMI).
- NIE WYSYŁAJ SWOJEGO ZDJĘCIA, PONIEWAŻ KTOŚ BĘDZIE MÓGŁ JE SKOPIOWAĆ, PRZEROBIĆ I PRZESŁAĆ DALEJ.
- BĄDŹ OSTROŻNY, JEŚLI CHCESZ SPOTKAĆ SIĘ Z OSOBAMI POZNANYMI PRZEZ INTERNET!
- NIE PODAWAJ NIKOMU DANYCH SWOICH ZNAJOMYCH.

ZAGROŻENIA PRZY PŁACENIU KARTĄ

- WIRUS INFEKUJE NASZE URZĄDZENIE, A NASTĘPNIE GROMADZI WSZYSTKIE DANE ZWIĄZANE Z PŁATNOŚCIAMI LUB NAWET PRZEPROWADZA TRANSAKCJE FINANSOWE W NASZYM IMIENIU
- KRADZIEŻ DANYCH DO BANKOWOŚCI ELEKTRONICZNEJ – PRZESTĘPCY PRÓBUJĄ UKRAŚĆ NASZE IMIĘ I NAZWISKO, ADRES, NUMER KARTY KREDYTOWEJ ORAZ PESEL
- NAJBEZPIECZNIEJSZE METODY PŁATNOŚCI ONLINE TO BEZPOŚREDNIE WPŁATY NA KONTO BANKOWE, KARTY BANKOWE (KREDYTOWE I DEBETOWE) ORAZ PORTFELE CYFROWE.

JAK ZAPOBIEC WŁAMANIU SIĘ NA KONTO?

- ZADBAJ O **SILNE HASŁA**
- PRZECHOWUJ HASŁA W BEZPIECZNYM MIEJSCU
- NIE ZOSTAWIAJ SWOJEJ KARTY BEZ NADZORU (NP. NIE POZWÓL, ABY KELNER ODSZEDŁ Z TWOJĄ KARTĄ PŁATNICZĄ, GDYŻ MOŻE SCZYTAĆ TWOJE DANE)

PHISHING – KRADZIEŻ DANYCH

PODSZYWANIE SIĘ POD OSOBY LUB INSTYTUCJE W CELU WYŁUDZENIA INFORMACJI, ZAINFEKOWANIA SPRZĘTU ZŁOŚLIWYM OPROGRAMOWANIEM LUB NAKŁONIENIA OFIARY DO OKREŚLONYCH DZIAŁAŃ.

JAK ROZPOZNAĆ PHISHING?

- BŁĘDY GRAMATYCZNE

JEDNĄ Z CZĘSTYCH (JESZCZE) OZNAK FAŁSZYWYCH WIADOMOŚCI SĄ BŁĘDY ORTOGRAFICZNE I NIEPOPRAWNA SKŁADNIA ZDANIA. BANKI I INNE DUŻE KORPORACJE DBAJĄ O SWOJĄ REPUTACJĘ, NIE DOPUSZCZAJĄC DO WYSTĘPOWANIA BŁĘDÓW ORTOGRAFICZNYCH I GRAMATYCZNYCH. ZAGRANICZNI OSZUŚCI KORZYSTAJĄ Z RÓŻNEGO RODZAJU TRANSLATORÓW. CO PRAWDA CORAZ LEPIEJ RADZĄ SOBIE ONE Z TŁUMACZENIAMI, JEDNAK NIE SPEŁNIAJĄ SWOJEJ ROLI W 100% I GENEROWANE PRZEZ NIE TREŚCI WYGLĄDAJĄ DOŚĆ SZTUCZNIE.

JAK ROZPOZNAĆ PHISHING?

- NIEZNANE, DŁUGIE ADRESY E-MAIL, NIETYPOWE TEMATY WIADOMOŚCI LUB WIADOMOŚCI BEZ TEMATÓW

ADRESY MAILOWE PRZYPOMINAJĄ POPRAWNE ADRESY. CYBERPRZESTĘPCY CELOWO STOSUJĄ **LITERÓWKI**, BY UZYSKAĆ NAZWĘ ADRESU ŁUDZĄCO PODOBNĄ DO ORYGINAŁU. CZASAMI ADRESY MAILOWE SĄ LOSOWO ROZDZIELANE PRZEZ KOMPUTERY I WÓWCZAS MOGĄ SKŁADAĆ SIĘ Z LOSOWYCH CYFR I LITER. W TAKIM PRZYPADKU ISTNIEJE BARDZO DUŻA SZANSA, ŻE MAMY DO CZYNIENIA Z TYPOWYM PHISHINGIEM.

JAK ROZPOZNAĆ PHISHING?

- GRA NA EMOCJACH

CYBERPRZESTĘPCY WYKORZYSTUJĄ LUDZKIE SŁABOŚCI LUB NIEUWAGĘ, BY OSIĄGNĄĆ KORZYŚĆ, NAJCZĘŚCIEJ FINANSOWĄ. ZA POMOCĄ MANIPULACJI DZIAŁAJĄ NA TAKIE EMOCJE JAK CIEKAWOŚĆ, UPRZEJMOŚĆ, POCZUCIE WINY, CHCIWOŚĆ, BEZMYŚLNOŚĆ CZY WSTYD. PRZESTĘPCY PODSZYWAJĄ SIĘ POD FIRMY, URZĘDY, OPERATORÓW TELEKOMUNIKACYJNYCH LUB NAWET NASZYCH ZNAJOMYCH, ABY WYŁUDZIĆ NASZE POUFNE DANE. DO NAJPOPULARNIEJSZYCH METOD NALEŻĄ INFORMACJE O NIEDOPŁACIE ZA PRZESYŁKĘ, ZALEGŁOŚCIACH ZA PRĄD, CZY PROŚBA O ZWERYFIKOWANIE DANYCH W ZWIĄZKU NP. Z TRZYNASTĄ EMERYTURĄ.

JEŚLI OTRZYMASZ PODEJRZANĄ WIADOMOŚĆ, NIE KLIKAJ W LINKI ANI NIE ODPOWIADAJ, DOPÓKI NIE POTWIERDZISZ AUTENTYCZNOŚCI NADAWCY.

BĄDŹ CZUJNY I DBAJ O SWOJE BEZPIECZEŃSTWO ONLINE!

DZIAŁANIE NA PSYCHIKĘ

FOMO

- W JĘZYKU ANGIELSKIM ROZWINIĘCIEM SKRÓTU FOMO JEST WYRAŻENIE **FEAR OF MISSING OUT**. OKREŚLA ONO SYTUACJĘ, W KTÓREJ OSOBA ODCZUWA PRZERAŹLIWY STRACH PRZED TYM, ŻE OMINIE JĄ JAKAŚ WAŻNA INFORMACJA I Z TEGO POWODU ODCZUWA POTRZEBĘ STAŁEGO MONITOROWANIA WYDARZEŃ PRZY UŻYCIU SMARTFONA CZY KOMPUTERA.
- PRZYJMUJE SIĘ, IŻ JEST TO GŁÓWNIE PROBLEM OSÓB MŁODYCH, KTÓRE W SIECI SPĘDZAJĄ MNÓSTWO CZASU. ZGODNIE Z DANYMI STATYSTYCZNYMI, NA SYNDROM FOMO MOŻE CIERPIEĆ AŻ **94 PROC**. OSÓB W WIEKU OD 15 DO 19 LAT. NIEMNIEJ JEDNAK CORAZ CZĘŚCIEJ DOTYCZY ON TAKŻE INNYCH GRUP WIEKOWYCH, W TYM EMERYTÓW.

NIEBIESKI WIELORYB

- GRA POWSTAŁA W ROSJI, NA ROSYJSKIM ODPOWIEDNIKU FACEBOOKA – PORTALU „VKONTAKTE”. ROZGRYWKA POLEGA NA WYPEŁNIANIU ZADAŃ. POŚRÓD 50 POLECEŃ MA BYĆ WYCINANIE NA CIELE PODOBIZN WIELORYBA, OGLĄDANIE PSYCHODELICZNYCH NAGRAŃ, SŁUCHANIE PRZYGNĘBIAJĄCEJ MUZYKI, A NA KOŃCU – SKOK Z WYSOKIEGO BUDYNKU.
- TO GRA W PARACH. OPIEKUN WYZNACZA ZADANIA, KTÓRE WYKONUJE DRUGA OSOBA ZWANA WIELORYBEM. PIERWSZE ZADANIE: WYCIĄĆ SOBIE COŚ ŻYLETKĄ NA RĘCE. OSTATNIE: SAMOBÓJSTWO.

MOMO

- MOMO TO W RZECZYWISTOŚCI RZEŹBA I ELEMENT WYSTAWY Z 2018 W VANILLA GALLERY W JAPONII. PRZERAŻAJĄCA POSTAĆ O WIELKIEJ GŁOWIE I TUŁOWIU PTAKA TO WYKREOWANA WIZJA ARTYSTYCZNA, JEDNAK JAKIMŚ CUDEM DZWONI ONA DO LUDZI I WYSYŁA ZDJĘCIA?!
- CO CIEKAWE, JAPOŃCZYK USTAWIŁ MOMO NA SWOJE ZDJĘCIE PROFILOWE W KOMUNIKATORZE WHATSAPP I WRZUCIŁ NUMER ZACZYNAJĄCY SIĘ OD LICZBY 81. TO WŁAŚNIE PRZY TEJ LICZBIE ZBIERA SIĘ NAJWIĘCEJ KONTROWERSJI, MÓWI SIĘ NAWET, ŻE JEST ONA PRZEKLĘTA. OKAZUJE SIĘ JEDNAK, ŻE LICZBA 81 TO... NUMER KIERUNKOWY DO JAPONII.
- LALKA WYSYŁA ZDJĘCIA, A KIEDY ZOSTAJE PRZYJĘTA DO GRONA ZNAJOMYCH, ZLECA ZADANIA DO REALIZACJI, KTÓRE MOGĄ DOPROWADZIĆ DO SAMOBÓJSTWA

FAKE NEWS

- NALEŻY ODRÓŻNIAĆ TAKIE NIEPRAWDZIWE I WPROWADZAJĄCE W BŁĄD TREŚCI OD SATYRY, PARODII I HUMORU. RÓWNIEŻ NIEKTÓRE OSOBY LUB INSTYTUCJE MOGĄ NAZYWAĆ FAKE NEWSAMI WIADOMOŚCI PRAWDZIWE Z POWODU NEGATYWNEJ DLA TYCH OSÓB LUB INSTYTUCJI ZAWARTOŚCI.
- FAKE NEWSY SĄ TWORZONE, A NASTĘPNIE ROZPOWSZECHNIANE, M.IN. Z POWODÓW POLITYCZNYCH, FINANSOWYCH, IDEOLOGICZNYCH (POGLĄDÓW I PRZEKONAŃ), A TAKŻE DLA ROZRYWKI, ZABAWY, Z CHĘCI ZWRÓCENIA NA SIEBIE UWAGI LUB UZYSKANIA ROZGŁOSU. SĄ ROZPOWSZECHNIANE W MEDIACH TRADYCYJNYCH I SPOŁECZNOŚCIOWYCH. CZĘSTO, W CELU PRZYCIĄGNIĘCIA UWAGI ODBIORCÓW, STOSOWANE SĄ W NICH CHWYTLIWE NAGŁÓWKI (ANG. **CLICKBAI**T).

BIBLIOGRAFIA

- HTTPS://POLSKABEZGOTOWKOWA.PL/DLA-CIEBIE/ARTYKULY/SKIMMING-CO-TO-JEST-I-JAK-SIE-PRZED-NIM-BRONIC/
- HTTPS://WWW.NEXERA.PL/PL/ARTICLES/JAK-ZADBAC-O-BEZPIECZENSTWO-SENIORA-W-INTERNECIE-159001699/
- HTTPS://WWW.KOMPUTERSWIAT.PL/ARTYKULY/REDAKCYJNE/ZAGROZENIA-W-INTERNECIE-20-NAJWIEKSZYCH-ZAGROZEN-INTERNETOWYCH/KBKE4KB
- HTTPS://BANK.PL/ZASADY-BEZPIECZNEGO-KORZYSTANIA-Z-INTERNETU-SA-TAKIE-SAME-DLA-WSZYSTKICH/

DZIĘKUJEMY ZA UWAGĘ