BIULETYN SZKOLNY

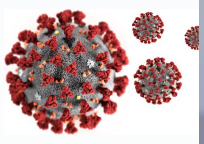
ZESPÓŁ SZKÓŁ IM. GEN. WŁADYSŁAWA SIKORSKIEGO W RUDNIKU NAD SANEM

WYDANIE SPECJALNE
MAJ 2020

ŚWIAT PRZED I ZA MONITOREM

„NIE WPADNIJ W SIEĆ"

KORONAWISUS CZY CYBERPRZESTZREŃ - CO NAM BARDZIEJ ZAGRAŻA?



Nauka i praca zdalna – sposobnością do oszustw!

Nasze życie ciągle się zmienia, lecz tego w jaki sposób się ono zmieniło w ostatnich miesiącach nikt z nas się nie spodziewał. Epidemia związana z koronawirusem spowodowała, że świat wstrzymał oddech, nasz styl życia się zmienił, zamknęły się drzwi szkół, kościołów, miejsc pracy i rozrywki.

Czy mieliśmy wybór? Nie! Ale mamy wybór odnośnie tego co robimy w cyberprzestrzeni.

Obecnie ogromna część naszego życia przeniosła się do Internetu. Uczymy się i pracujemy zdalnie, a większość spraw załatwiamy online. Sytuacja z COVID-19stała się narzędziem w rękach cyber-przestępców i cyberoszustów.

W ostatnim czasie nasilają się najpopularniejsze cyberzagrożenia – zwłaszcza ***phishing,*** czyli wyłudzanie danych, np. loginów i haseł do kont bankowych. Są coraz sprytniejsi i potrafią się coraz lepiej podszyć pod nadawcę, z którym wcześniej korespondowaliśmy, wykorzystując nawet autentyczne fragmenty wykradzionych wcześniej treści naszych maili. Jednak w większości przypadków oglądając uważnie wiadomość można dostrzec cechy, które powinny spowodować, że zapali się przysłowiowe ostrzegawcze światełko.

Oszuści wykorzystują socjotechnikę, element zaskoczenia i fakt, że pod wpływem emocji reagujemy instynktownie – zaciekawieni wiadomością klikniemy szybko w załączony link, który kieruje do fałszywej strony z płatnościami lub innej strony wymagającej podanie naszych danych. W ten sposób sami otwieramy przestępcom drzwi.

Wciąż są wykorzystywane znane już sposoby wyłudzeń pod pretekstem rzekomego *wycieku zdjęć*. Zaczyna się od przejęcia konta znajomego ofiary, a następnie z przejętego konta wychodzi seria wiadomości na Messengerze, do wszystkich osób na liście znajomych. W treści wiadomości, która jest na ogół napisana poprawnie w języku, czytamy dramatycznie brzmiące ostrzeżenie o rzekomym wycieku naszych prywatnych zdjęć. Wtedy odruchowo i w emocjach wchodzimy na stronę, szybko się na niej logujemy i... oddajemy w ten sposób login i hasło przestępcom. Popularne sieci , jak np. Orange Polska zablokowała w ciągu jednego tygodnia aż 241 takich fałszywych witryn.

Bądź ostrożny w sieci i chroń siebie. Nie korzystaj z publicznych sieci WiFi, zawsze wybierajmy w pełni bezpieczne połączenie. Sprawdzaj autentyczność otrzymywanych wiadomości, zwracaj uwagę na nadawcę, treść – szczególnie na błędy w pisowni lub te, które ewidentnie wynikają ze złego tłumaczenia. Instalując aplikacje na smartfonie, pobieraj je tylko z certyfikowanych sklepów.

W tym numerze

Ważne tematy

- BEZPIECZEŃSTWO W SIECI
- CYBERPRZEMOC
- OSZUSTWA INTERNETOWE

EKRAN MONITORA— ZAMIAST TWARZY DRUGIEGO CZŁOWIEKA

Od dłuższego czasu zmagamy się z uzależnieniem od ekranu. Tymczasem sytuacja sprawiła, że zostaliśmy przykuci do internetu, nowych mediów jak nigdy wcześniej. Tak pracujemy, uczymy, korzystamy ze świata.

Co na ten temat sądzi dr Maciej Dębski - socjologi, badacz i Prezes Fundacji DBAM O MÓJ Z@SIĘG ?

Posłuchaj wypowiedzi z dnia 10.04.2020 na temat:

Naukowcy o wpływie ekranu w czasach koronawirusa

RADIO KRAKÓW:

http://www.radiokrakow.pl/audycje/rozmowy-przed-hejnalem/

ZŁOŚLIWY SPAM— link w wirusem

Od początku roku zarejestrowano ponad 4 tys. domen internetowych, które swoją treścią nawiązują do koronawirusa. 3% z nich zostało zidentyfikowanych jako złośliwe, a dalsze 5 % jako wzbudzające podejrzenia – informuje Check Point Threat Intelligence.

KORONO Hak-erzy

CERT Polska (zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet, istniejący od 1996) informował o ataku mającym na celu pozyskanie dostępu do konta Facebook i wyłudzanie kodów BLIK od znajomych, tym razem ze scenariuszem informacji o koronawirusie. Schemat ataku jest niezmienny od dłuższego czasu: istnieje strona z sensacyjnym fake newsem (koronawirus, porwanie dziecka, wypadek samochodowy z udziałem dziecka) podszywającym się pod portal informacyjny, stronę policji czy stacji TV. Na samym końcu strony znajduje się nagranie z kamery, które wymaga podania przez ofiarę danych logowania do serwisu Facebook. W roku 2019 CERT Polska prowadził działania w sprawie 224 fałszywych stron logowania do Facebooka, a od początku roku 2020 odnotowano już 236 przypadków.

TECHNOLOGIA I MY
współpraca czy walka?

Sytuacja z COVID-19 spowodowała, że nauka, praca, procesy biznesowe i interakcje międzyludzkie przeniosły się do sfery cyfrowej.

Nasz ŚWIAT stał się pełen technologii informacyjno-komunikacyjnych.

Typowe cechy współczesnych technologii to:

1. **Powszechność** - na świecie jest obecnie 7,7 mld osób z czego 4,5 mld używa Internetu, ponad 5 mld używa portali społecznościowych i komunikatorów. W Polsce jest to odpowiedni 38 mln osób z czego 30 mln użytkowników Internetu. Liczba użytkowników się powiększa.
2. **Wpływ na zdrowie**— nowe technologie i ich użytkowanie ma negatywny lub pozytywny wpływ na nasze życie, funkcjonowanie i zdrowie – w ujęciu fizycznym psychicznym, społecznym i duchowym.
3. **Przydatność**—używanie nowych technologii jak pokazuje obecna sytuacja w dobie pandemii COVID-19 jest przydatne – dzięki odpowiedniemu używaniu internetu, komputera, telefonu, a nawet gier cyfrowych jesteśmy w stanie podnosić swoje kompetencje edukacyjne czy społeczne.
4. **Reduktor stresu i dostawca przyjemności**—używanie nowych technologii jest związane z jednej strony z przyjemnością, a z drugiej strony to dokonały reduktor stresu.

Warto pamiętać, że smartfony mają być dla nas wsparciem w nauce, pracy i dostarczać rozrywki. Człowiek nie może spędzać jednak całego czasu w pracy, szkole lub na zabawie. Cyfrowa Higiena polega również na dostrzeganiu tego aspektu i żaden, nawet najmądrzejszy program, nie wypracuje jej za nas.

UZALEŻNIENIE

Wśród specjalistów brak jednoznacznej zgody czy powinno się mówić o "nadużywaniu Internetu", czy wręcz o „uzależnieniu" od Internetu. Nie sposób jednak zaprzeczyć, że nadmierne korzystanie z Internetu jest coraz bardziej powszechnym zjawiskiem. Chociaż z pojęciem nadużywania komputera i/lub Internetu kojarzyć się mogą nagłaśniane przez media przypadki śmierci w efekcie spędzenia kilkudziesięciu godzin non-stop przed komputerem, dużo bardziej powszechne są sytuacje, w których dochodzi do dezorganizacji życia, problemów z nauką, zaniedbania dotychczasowych zainteresowań na skutek intensywnego korzystania z gier sieciowych.
W sytuacji, kiedy Internet zdominował komunikację i dostęp do informacji, trudno wyznaczyć jednoznaczne kryteria pozwalające na odróżnienie „normalnego" od „patologicznego" korzystania z sieci i komputera. Miarą nie może być jedynie czas spędzany w Internecie, bo większe znaczenie ma jego jakość – to, na co dziecko przeznacza ten czas. Jednak właśnie długie godziny spędzone przed komputerem mogą być pierwszym sygnałem alarmowym, skłaniającym rodziców do zwrócenia uwagi na dziecko. **Jako kryteria wskazujące na pojawienie się problemu przyjmuje się (za dr. n. med. Bohdanem Woronowiczem z Instytutu Psychiatrii i Neurologii oraz Centrum AKMED w Warszawie):**

- spędzanie przy komputerze coraz więcej czasu kosztem innych zainteresowań;
- zaniedbywanie obowiązków rodzinnych i szkolnych z powodu aktywności w Internecie;
- pojawianie się konfliktów rodzinnych związanych z Internetem;
- kłamstwa dotyczące czasu spędzanego w Internecie;
- podejmowanie nieudanych prób ograniczenia czasu spędzonego przed komputerem;
- reagowanie rozdrażnieniem lub nawet agresją, gdy korzystanie z komputera jest utrudnione lub niemożliwe.

Korzystanie z Internetu to pojęcie bardzo ogólne. Patologiczne użytkowanie sieci może szczególnie dotyczyć jednej lub kilku form aktywności online:

- gry internetowe (zwłaszcza te pozwalające na rywalizację online z innymi użytkownikami);
-aktywność na portalach społecznościowych;
-pornografia, cyberseks.

HIGIENA W SIECI- jej znaczenie

Używanie nowych technologii w sposób niehigieniczny, nadużywający, uzależniający— **to BŁĄD**

ZDROWE ZACHOWANIA—MOGĄ STAĆ SIĘ ZŁYMI NAŁOGAMI

WIEMY ŻE:

- Obecna młodzież i dzieci to pokolenie cyfrowe
- To nie media cyfrowe są złe! Niewłaściwe może być ich używanie
- Pozytywne lub negatywne mogą być nasze motywacje i wzory używania nowych technologii
- Istnieje potrzeba przekazywania kreatywnych komunikatów używania nowych technologii
- Nadużywanie lub uzależnianie się od nowych technologii wynika z głębszych problemów lub sytuacji np. brak odpowiedniej komunikacji z rodzicami, kolegami czy nauczycielami
- Zachowania podejmowanie w przestrzeni Internetu mają takie same skutki jak zachowania podejmowane poza siecią
- Świat online i offline jest mocno zazębiony— odzwierciedla NAS

HIGIENA CYFROWA– OPCJA W TWOIM TELEFONIE, KTÓRA WSPIERA TWOJĄ NORMANOŚĆ

Ty sterujesz telefonem, a nie on tobą

DOWIEDZ SIĘ WIĘCEJ!

Czym jest cyberprzemoc?

Cyberprzemoc to inaczej przemoc z użyciem mediów elektronicznych – przede wszystkim Internetu i telefonów komórkowych.
Problem ten dotyczy przede wszystkim dzieci i młodzieży. W Polsce doświadcza go ponad połowa młodych internautów!!!

Do działań określanych jako cyberprzemoc zalicza się m.in:

- wyzywanie, straszenie poniżanie kogoś w Internecie lub przy użyciu telefonu,
- robienie komuś zdjęć lub rejestrowanie filmów bez jego zgody,
- publikowanie w Internecie lub rozsyłanie telefonem zdjęć, filmów lub tekstów, które kogoś obrażają lub ośmieszają,
- podszywanie się pod kogoś w Sieci.

Pomimo, że akty cyberprzemocy mogą wyglądać niewinnie, to potrafią wyrządzać bardzo dużą krzywdę.

Zasady bezpieczeństwa!

1. Zanim dołączysz
Kontakty z ludźmi na portalach społecznościowych, podobnie jak kontakty z ludźmi w świecie rzeczywistym, rządzą się pewnymi zasadami. Zastanów się w jaki sposób działa portal zanim utworzysz na nim swój profil. Przede wszystkim zainteresuj się jaki poziom prywatności gwarantuje Ci dany portal. Informacji tego typu szukaj w regulaminie, który powinien jasno określać zasady twojego uczestnictwa w serwisie.
2. Prywatność
Kontroluj dostęp do Twoich danych i innych informacji, które umieszczasz w swoim profilu. Bezpieczny portal społecznościowy powinien pozwolić Ci nadać sobie taki status prywatności, który zagwarantuje, że informację o Tobie będą dostępne tylko dla znajomych, których świadomie dodałeś/aś do swojej listy. Pamiętaj też, że Twoje hasło to Twój sekret.
3. Informacje o mnie
Zamieszczając informacje o sobie pamiętaj, że potencjalnie każdy może je zobaczyć. Dbaj o to, żeby nie ujawniać swoich danych osobowych. Stwórz bezpieczny Nick, który nie zdradzi Twojej prawdziwej tożsamości. Sieć daje nam możliwość bycia kimś innymi niż w codziennym życiu. Znaj jednak swoje granice tej zabawy - myśl jak się prezentujesz.
4. Zdjęcia
Zastanów się dobrze zanim zamieścisz w Sieci swoje zdjęcia, które mogą być użyte, przez innych użytkowników Sieci, w sposób jakiego byś sobie nie życzył/a lub skopiowane do miejsca, w którym byś ich nie zamieścił/a. Jeżeli już na pewno chcesz zamieścić swoje zdjęcia w Internecie ustaw taki status prywatności, który zagwarantuje Ci bezpieczeństwo.
5. Kontakty z innymi
Bądź czujny/a w kontaktach z osobami znanymi wyłącznie Sieci. Flirt z nieznajomym/ą może być dobrą zabawą, ale może też mieć niebezpieczne konsekwencje. W Sieci ludzie często udają kogoś kim nie są ukrywając w ten sposób swoje prawdziwe intencje. Bądź bardzo ostrożny/a, jeżeli nowy internetowy „przyjaciel" chce się z Tobą spotkać w realu. Jeżeli zdecydujesz się na spotkanie, spotkaj się w miejscu publicznym (centrum handlowym czy w ruchliwej kawiarni) a na spotkanie pójdź z kimś, komu ufasz. Powiedz o planowanym spotkaniu odpowiedzialnej osobie dorosłej.
6. Odpowiedzialność za informacje
Jeżeli piszesz coś w Internecie będąc pod wpływem silnych emocji, przeczytaj to dwa razy. Daj sobie czas żeby się uspokoić i sprawdź czy to, co planujesz wysłać jest tego warte.
Twojej korespondencji i Twoich działań w Sieci. Dlatego, w Sieci, nie pisz nigdy czegoś, czego nie napisałbyś/abyś na kartce pocztowej, którą nie tylko bezpośredni adresat może przeczytać.
Pamiętaj też, że ludzie przesyłają dalej, upubliczniając wiadomości. Sam/a także zawsze patrz, co przesyłasz dalej. Nie ujawniaj danych innych osób – nie przesyłaj dalej cudzych maili i nie podawaj w Sieci danych innej osoby bez jej zgody.

MOŻESZ TO ZMIENIĆ

REAGUJEMY PRZECIWKO PRZEMOCY

⇒ **Szanuj innych**
Bądź miły/a dla innych w Sieci. Zastanów się czy adresat życzyłby sobie zobaczyć taki wpis i czy Ty powiedziałbyś/abyś lub pokazał/a to samo podczas spotkania twarzą w twarz?
Poczucie humoru, poglądy i zasady innych ludzi bywają różne także w Sieci. Respektuj innych w Internecie, a jeżeli kogoś urazisz znajdź metodę, żeby sprawę wyjaśnić i go przeprosić.
Jeżeli ktoś Ciebie obraża myśląc, że zrobiłeś/aś coś niemiłego celowo – zamiast dać się ponieść emocjom, spróbuj wyjaśnić, że to nie było celowe, że to wynik nieporozumienia.

⇒ **Działaj mądrze**
Ktoś Cię prowokuje? Nie daj mu satysfakcji. Zazwyczaj jest to metoda na zwrócenie na siebie uwagi, jeżeli takiego kogoś zignorujesz prawdopodobnie da Ci spokój.

⇒ **Pomoc**
Masz prawo do godności w Internecie. Jeżeli jesteś atakowany/a, ktoś Cię straszy lub grozi Ci działaj w swojej obronie. Zgłoś fakt cyberprzemocy odpowiednim instytucjom (szkoła, policja, helpline.org.pl – 0-800-100-100) i osobom, które mogą Ci udzielić pomocy: rodzice, pedagog szkolny, nauczyciel. Razem szybko i skutecznie rozwiążecie problem.

⇒ **Pamiętaj o realu**
Internet jest fajny, ale nie zapominaj o realnym świecie. Kontroluj to, ile czasu spędzasz w Sieci. Dbaj o kontakty z ludźmi w świecie rzeczywistym. Nawet mając pięciuset znajomych na portalu społecznościowym możesz czuć się samotnym/ą. Nic nie zastąpi prawdziwych znajomości.

⇒ **Gdzie szukać pomocy**
Jeżeli ktoś nęka Cię w Sieci, nabija się z Ciebie, wysyła obraźliwe e-maile, sms'y, zadaje Ci na czacie, w mailu lub przez komunikator jakieś krępujące pytania, wypytuje Cię o prywatne dane, nalega na spotkanie…

...skontaktuj się z Helpline.org.pl.
Wejdź na stronę www.helpline.org.pl i skorzystaj z komunikatora, lub zadzwoń pod bezpłatny numer **0 800 100 100.**

OCHRONA PRAWNA

Formy cyberprzemocy	Działania	Artykuł
Wulgarne wyzywanie	Publikacja nieprzyzwoitych treści, zdjęcia, rysunku, obrazu	Kodeks wykroczeń Art. 141
Poniżanie, ośmieszanie, upokarzanie	Uporczywe nękanie	Kodeks wykroczeń Art. 107 Kodeks karny Art. 190a
Straszenie, szantaż	Groźby	Kodeks karny Art. 190&1-2 i 191&1-2
Niechciane zdjęcia i filmy	Naruszenie wizerunku	Kodeks cywilny Art. 23 i 24
Publikacja kompromitujących materiałów	Naruszenie czci (zniesławienie, znieważenie)	Kodeks karny Art. 212&1-4
Podszywanie się	Włamania do miejsca strzeżonego hasłem lub innym zabezpieczeniem	Kodeks karny Art. 267&1-4, 268a&1-3 , 190a&2

CHROŃ SIEBIE, SWOICH KOLEGÓW, SWOICH NAUCZYCIELI—

Powiedz STOP—TO JEST TWOJA MOC

Cyberprzemoc podczas e-lekcji

Rajdy na lekcje online

Użytkownicy internetu często spotykają się z cyberprzemocą. W czasie trwania pandemii, gdy edukacja przeniosła się do sieci, z tą formą prześladowania zmaga się coraz więcej nauczycieli. Teraz patostremerzy obrali sobie za cel uniemożliwienie nauczycielom prowadzenia e-lekcji. Podszywając się pod uczniów, włamują się na zajęcia i w wulgarny sposób zakłócają ich przebieg. Udostępniają patotreści i atakują uczestników. Ich hejterskie wystąpienia uderzają zarówno w nauczycieli, jak i w uczniów. Często nagrania z takiej zakłóconej lekcji trafiają do sieci. Rajdowanie to bardzo agresywna forma przemocy internetowej. Atakujący nie tylko osiągają cel – uniemożliwienie prowadzenia lekcji online – ale dodatkowo prześladują nauczycieli i uczniów.

Rajd na e-lekcje— to m.in. trolling, bombing, uciążliwe przeszkadzanie, a niejednokrotnie uniemożliwianie przeprowadzenia spotkania.

Bezpieczne e-lekcje

Rzecznik Praw Obywatelskich oraz Ministerstwo Cyfryzacji stanowczo sprzeciwiają się działaniom patostremarów i rajdowaniu lekcji. Dlatego podejmują kroki, aby walczyć z tym procederem.

Ministerstwo Cyfryzacji podjęło współpracę z przedstawicielami platform społecznościowych i komunikacyjnych oraz Biura do Walki z Cyberprzestępczością w Komendzie Głównej Policji. „Bezpieczeństwo w sieci dzieci, młodzieży i nauczycieli jest dla nas priorytetem" – podkreśla Ministerstwo Cyfryzacji.

PAMIĘTAJ!

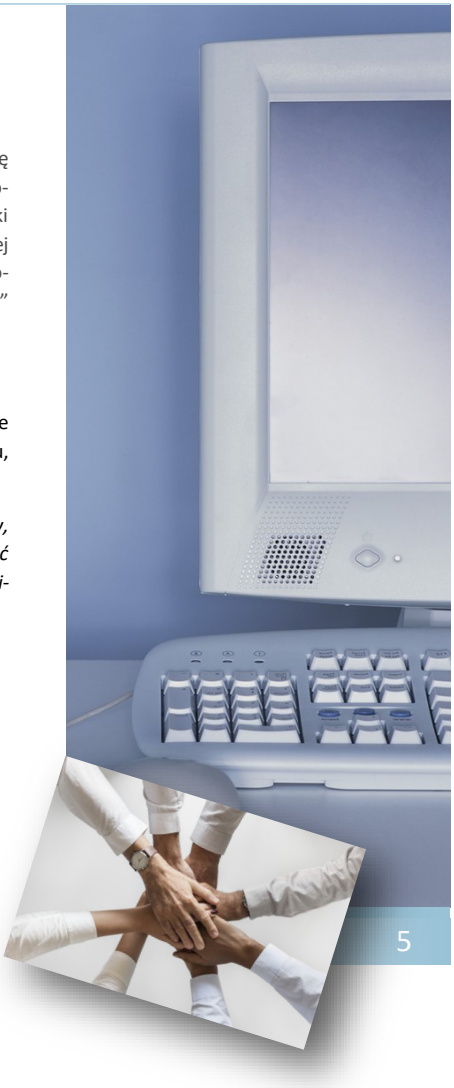
Prawa nauczycieli prowadzących lekcje on-line dotyczące danych osobowych, wizerunku, dobrego imienia są *CHRONIONE.*

W Internecie nikt nie jest anonimowy, a sprawcy takich zachowań, mogą spodziewać się surowych konsekwencji – mówi wiceminister Adam Andruszkiewicz.

Nie daj się cyberprzemocy

Nauczycielu—to w jaki sposób zareagujesz na cyberprzemoc wpłynie na zachowanie agresora. Dlatego ważne jest, aby reakcja była stanowcza, ale i odpowiednia do danej sytuacji.

- **ROZMAWIAJ Z UCZNIAMI**
- **W RAZIE KONIECZNOŚCI ZGŁOŚ ORGANOM ŚCIGANIA**



Lubię! #niehejtuje - Kampania społeczna Reporter Young
https://www.signs.pl/lubie%21-niehejtuje---kampania-spoleczna-reporter-young,382719,artykul.html

DLACZEGO PRZEBYWAM W SIECI? - DRUGIE DNO

Pamiętaj

Zdaniem lekarzy i psychologów, ucieczka w Internet to często jedynie objaw głębszych problemów. Problemami maskowanymi ucieczką w wirtualny świat mogą być m.in.: depresja, neurotyzm, nieśmiałość, współwystępowanie innych nałogów, niska samoocena, negatywne strategie radzenia sobie ze stresem. W tym przypadku niezbędna może być terapia psychologiczna.

W przypadku nadużywania Internetu rozwiązaniem nie jest na pewno odcięcie dostępu do sieci (o ile nadużywanie komputera nie zagraża bezpośrednio życiu lub zdrowiu).

Znajdziesz i tak dostęp do sieci – w szkole lub u kolegi. Dużo większe znaczenie ma zmiana TWOICH postaw wobec Internetu – z „zabijania czasu" na bardziej konstruktywne, służące edukacji i rozwojowi TWOICH zainteresowań.

Bezpieczeństwo młodzieży w sieci

Na stronie internetowej Podkarpackiej Policji znajdziesz wszystkie niezbędne informacje związane z bezpieczeństwem w sieci .

Link: http://www.podkarpacka.policja.gov.pl/rze/komendy-policji/kpp-nisko/komunikaty/97757,Bezpieczenstwo-mlodziezy-wsieci.html

W artykule zamieszczono informacje o tym, co powinno obudzić naszą czujność w związku z przebywaniem w cyberprzestrzeni, m.in. phishing, „robaki" i pharming, a także zalecenia dotyczące bezpiecznego korzystania z sieci, pilnowania swoich haseł i zakupów w Internecie „bez strat".

ZAPOZNAJ SIĘ !
INFORMACJE TE ZOSTAŁY PRZEKAZANE W TROSTE O TWOJE BEZPIECZEŃSTWO.

Dziękujemy za wsparcie Komendzie Powiatowej Policji w Nisku.

Opracowanie:
mgr Monika Reichert

Konsultacja merytoryczna:
mgr Sylwia Matyka - pedagog

aspirant sztabowy
Bernard Dul - Komenda Powiatowa Policji w Nisku

WYDANIE SPECJALNE BIULETYNU
ZESPOŁU SZKÓŁ IM. GEN . WŁADYSŁAWA SIKORSKIEGO
W RUDNIKU NAD SANEM

ZOSTAŁO OPRACOWANE W RAMCH
AKCJI INFORMACYJNO-PROFILAKCTYCZNEJ
Z ZAKRESU BEZPIECZNEGO UŻYTKOWANIA TECHNOLOGII
INFORMACYJNO-KOMPUTEROWYCH I CYBERPRZEMOCY