



RAPORT NORTON 2013

RAPORT NORTON 2013

24 KRAJE

ARABIA SAUDYJSKA, AUSTRALIA, BRAZYLIA, CHINY, DANIA, FRANCJA,
HOLANDIA, INDIE, JAPONIA, KANADA, KOLUMBIA, MEKSYK, NIEMCY, NOWA
ZELANDIA, POLSKA, ROSJA, RPA, SINGAPUR, STANY ZJEDNOCZONE,
SZWECJA, TURCJA, WIELKA BRYTANIA, WŁOCHY, ZJEDNOCZONE EMIRATY
ARABSKIE

13022 DOROSŁYCH INTERNAUTÓW W WIEKU OD 18 DO 64 LAT

KTO NAJCZĘŚCIEJ PADA OFIARĄ CYBERPRZESTĘPCÓW?

OFIARY PRZESTĘPCÓW W
INTERNECIE TO ZWYKLE:

MĘŻCZYŹNI  – **64%**

66% 

(DLA PORÓWNANIA: KOBIETY – 58%)

POKOLENIE Y – **66%**

70% 

(DLA PORÓWNANIA: POKOLENIE WYŻU PO II WOJNIE
ŚWIATOWEJ – 54%)

ORAZ

- UŻYTKOWNICY URZĄDZEŃ MOBILNYCH – **63%**
- UŻYTKOWNICY SIECI SPOŁECZNOŚCIOWYCH – **63%**
- UŻYTKOWNICY PUBLICZNYCH/NIEZABEZPIECZONYCH
SIECI WI-FI – **68%**
- MIESZKAŃCY KRAJÓW ROZWIJAJĄCYCH SIĘ – **68%**
- RODZICE DZIECI W WIEKU OD 8 DO 17 LAT – **65%**

NAJWIĘCEJ OFIARY
CYBERPRZESTĘPCÓW:



ROSJA

85%



CHINY

77%



RPA

73%

GŁÓWNE ZAGADNIENIA

UŻYTKOWNICY TABLETÓW I SMARTFONÓW ZANIEDBUJĄ BEZPIECZEŃSTWO

PRAWIE POŁOWA NIE STOSUJE NA SWOICH URZĄDZENIACH MOBILNYCH PODSTAWOWYCH ZABEZPIECZEŃ, TAKICH JAK HASŁA, OPROGRAMOWANIE OCHRONNE CZY KOPIE ZAPASOWE PLIKÓW. PONAD JEDNA TRZECIA DOŚWIADCZYŁA W UBIEGŁYM ROKU MOBILNEJ CYBERPRZESTĘPCZOŚCI.

KOSZTY CYBERPRZESTĘPCZOŚCI DOTYKAJĄCEJ UŻYTKOWNIKÓW INDYWIDUALNYCH

GLOBALNIE WYNOSZĄ 113 MLD USD ROCZNIE — KOSZT PRZYPADAJĄCY NA OFIARĘ CYBERPRZESTĘPCZOŚCI WZRÓSŁ O 50%.

SKALA CYBERPRZESTĘPCZOŚCI WOBEC KONSUMENTÓW

PONAD MILION OFIAR DZIENNIE

ROZMYCIE SIĘ GRANIC MIĘDZY PRACĄ A ZABAWĄ STWARZA OKAZJE DLA PRZESTĘPCÓW

GLOBALNIE 49% UŻYTKOWNIKÓW WYKORZYSTUJE SWOJE PRYWATNE URZĄDZENIA DO PRACY I ZABAWY. MNIEJ WIĘCEJ JEDEN NA PIĘCIU UDOSTĘPNIŁ INFORMACJE ZWIĄZANE Z PRACĄ SWOIM PRZYJACIOŁOM I RODZINIE.

UŻYTKOWNICY SMARTFONÓW I TABLETÓW ZANIEDBUJĄ BEZPIECZEŃSTWO

NIEMAL **1/2** UŻYTKOWNIKÓW SMARTFONÓW/TABLETÓW ŚPI ZE
SWOIM URZĄDZENIEM W ZASIĘGU RĘKI

NIEMAL **1/2** NIE STOSUJE NA SWOICH URZĄDZENIACH
MOBILNYCH PODSTAWOWYCH ŚRODKÓW OSTROŻNOŚCI, TAKICH JAK
HASŁA, OPROGRAMOWANIE ZABEZPIECZAJĄCE CZY KOPIE ZAPASOWE
PLIKÓW*

TYLKO **26%** UŻYTKOWNIKÓW SMARTFONÓW
DYSPONUJE ZAAWANSOWANYM OPROGRAMOWANIEM
ZABEZPIECZAJĄCYM



57% NIE ZDAJE SOBIE SPRAWY Z ISTNIENIA OPROGRAMOWANIA
ZABEZPIECZAJĄCEGO DLA URZĄDZEŃ MOBILNYCH*. W POLSCE **59%**



STAN WIEDZY O ZABEZPIECZENIACH — WYSOKI W PRZYPADKU PC, NISKI DLA URZĄDZEŃ MOBILNYCH

USUWA PODEJRZANE
WIADOMOŚCI E-MAIL OD
NIEZNANYCH NADAWCÓW

 **90%**

VS.

 **60%**


VS.


 **56%**
50% 

MA CO NAJMNIEJ
PODSTAWOWY, BEZPŁATNY
PROGRAM ANTYWIRUSOWY

72%

VS.

42%
50% 
VS.


33%
28% 

UNIKA PRZECHOWYWANIA
POUFNYCH PLIKÓW ONLINE

78%

VS.

53%
VS.

48%
50% 



CYBERPRZESTĘPCZOŚĆ MOBILNA I STRATY

38% UŻYTKOWNIKÓW SMARTFONÓW

DOŚWIADCZYŁO MOBILNEJ CYBERPRZESTĘPCZOŚCI W
CIAGU OSTATNICH 12 MIESIĘCY*

36% 

27% DOROSŁYCH ZGUBIŁO SWOJE URZĄDZENIE

MOBILNE LUB MIAŁO DO CZYNNIENIA Z JEGO KRADZIEŻĄ

22% 



KOSZTY CYBERPRZESTĘPCZOŚCI DOTYKAJĄCEJ UŻYTKOWNIKÓW INDYWIDUALNYCH

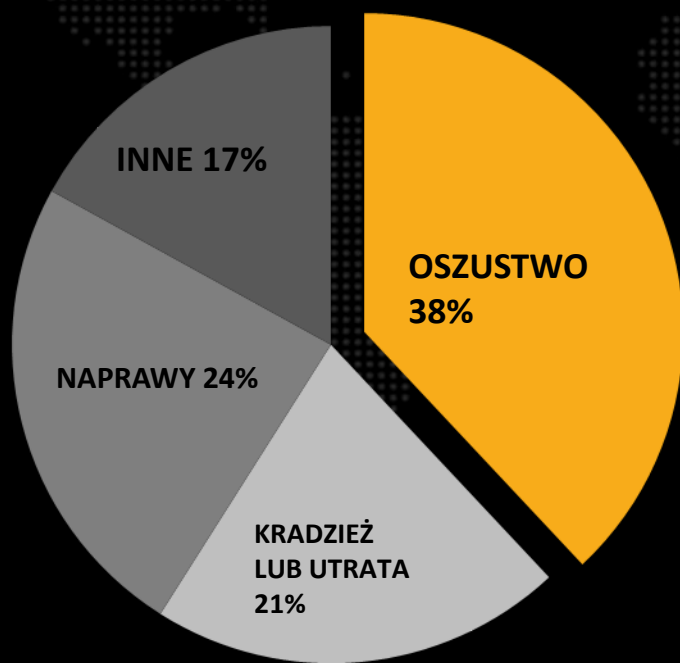
113 MLD USD

6 MLD PLN 

TO DOŚĆ, ABY PRAWIE 10 RAZY ZORGANIZOWAĆ IGRZYSKA OLIMPIJSKIE W LONDYNIE Z 2012 R.



83% KOSZTÓW BEZPOŚREDNICH TO EFEKT OSZUSTW, KRADZIEŻY I STRAT ORAZ NIEZBĘDNYCH NAPRAW



298 USD

983 PLN 

ŚREDNI KOSZT NA OFIARĘ

GLOBALNIE TO 50% WZROST W STOSUNKU DO 2012 R.

WSZYSTKIE KWOTY W USD

PATRZ OBLICZENIA EKSTRAPOLACYJNE*

KOSZTY CYBERPRZESTĘPCZOŚCI DOTYKAJĄCEJ UŻYTKOWNIKÓW INDYWIDUALNYCH



38 USA
MLD



3 MEKSYK
MLD



8 BRAZYLIA
MLD



2 POLSKA
MLD



12 EUROPA
MLD



1 ROSJA
MLD



4 INDIE
MLD



37 CHINY
MLD



1 JAPONIA
MLD



1 AUSTRALIA
MLD



0,3 RPA
MLD

WSZYSTKIE KWOTY W USD ZAOKRĄGLONO DO PEŁNEGO MILIARDA

KANADA 3 MLD; SINGAPUR 1 MLD; NOWA ZELANDIA 0,1 MLD; TURCJA 2 MLD; ARABIA SAUDYJSKA 0,5 MLD; ZEA 0,3 MLD; KOLUMBIA 0,5 MLD

SKALA CYBERPRZESTĘPCZOŚCI WOBEC KONSUMENTÓW

378 MILIONÓW OFIAR ROCZNIE 

NIEMAL 2,8 RAZY WIĘCEJ NIŻ LICZBA DZIECI PRZYCHODZĄCYCH NA ŚWIAT W CIĄGU ROKU

6 MILIONÓW OFIAR ROCZNIE W POLSCE 



1 MILION +
OFIAR DZIENNIE

WYSTARCZY, ABY WYPEŁNIĆ STADION WEMBLEY (ANGLIA) PONAD 10 RAZY



12 OFIAR NA SEKUNDĘ

SKALA CYBERPRZESTĘPCZOŚCI WOBEC KONSUMENTÓW



**50% DOROSŁYCH
INTERNAUTÓW**

PADŁO W UBIEGŁYM ROKU OFIARĄ CYBERPRZESTĘPCZOŚCI
I/LUB NAPOTKAŁO NEGATYWNE SYTUACJE ONLINE
(NP. OTRZYMAŁO NAGIE ZDJĘCIA OD OBCYCH LUB BYŁO
ZASTRASZANYCH ALBO NĘKANYCH ONLINE)

49% W POLSCE 

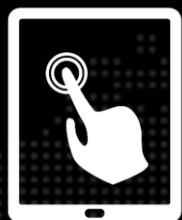
41% DOROSŁYCH INTERNAUTÓW


PADŁO OFIARĄ SZKODLIWEGO OPROGRAMOWANIA, WIRUSÓW
HAKERÓW, A TAKŻE OSZUSTW I KRADZIEŻY

40% W POLSCE 





ZACIERANIE SIĘ GRANIC MIĘDZY PRACĄ I ZABAWĄ





49% UŻYTKOWNIKÓW WYKORZYSTUJE SWOJE PRYWATNE URZĄDZENIA DO PRACY I ZABAWY*. W POLSCE **43%** 

36% TWIERDZI, ŻE ICH FIRMA NIE DYSPONUJE POLITYKĄ DOTYCZĄCĄ WYKORZYSTYWANIA URZĄDZEŃ PRYWATNYCH DO CELÓW SŁUŻBOWYCH*. W POLSCE **45%** 

30% RODZICÓW POZWALA SWOIM DZIECIOM BAWIĆ SIĘ, POBIERAĆ PLIKI I ROBIĆ ZAKUPY ZA POMOCĄ ICH SŁUŻBOWYCH URZĄDZEŃ**. W POLSCE **21%** 

49%  **46%** 
RESPONDENTÓW ODCZYTUJE LUB WYSYŁA PRYWATNE EMAILE ZA POMOCĄ URZĄDZEŃ SŁUŻBOWYCH*

34%  **28%** 
KORZYSTA Z MEDIÓW SPOŁECZNOŚCIOWYCH NA URZĄDZENIACH SŁUŻBOWYCH*

27%  **23%** 
PRZECHOWUJE INFORMACJE PRYWATNE NA SWOICH URZĄDZENIACH SŁUŻBOWYCH*

*WSRÓD PRACUJĄCYCH OSÓB DOROSŁYCH

**WSRÓD RODZICÓW, KTÓRZY KORZYSTAJĄ Z URZĄDZEŃ UDOSTĘPNIONYCH IM PRZEZ PRACODAWCĘ

PRZECHOWYWANIE PLIKÓW W SIECI



24% UŻYTKOWNIKÓW ZAPISUJE SŁUŻBOWE I PRYWATNE PLIKI NA TYM SAMYM KONCIE ONLINE. W POLSCE **17%** 

WŚRÓD OSÓB UDOSTĘPNIAJĄCYCH INFORMACJE ZWIĄZANE Z PRACĄ NA STRONACH DO PRZECHOWYWANIA PLIKÓW:

18% UDOSTĘPNIĄ JE ZNAJOMYM

10% 

21% UDOSTĘPNIĄ JE RODZINIE

14% 

WYSTAWIAJĄ TYM SAMYM NA RYZYKO ZARÓWNO SŁUŻBOWE, JAK I PRYWATNE DOKUMENTY.

RYZYKOWNE ZACHOWANIA W MEDIACH SPOŁECZNOŚCIOWYCH



39% 36% 

UŻYTKOWNIKÓW SERWISÓW
SPOŁECZNOŚCIOWYCH NIE
WYLOGOWUJE SIĘ PO KAŻDEJ
SESJI



1/4 3/10 

UŻYTKOWNIKÓW MEDIÓW
SPOŁECZNOŚCIOWYCH
PRZEKAZUJE SVOJE HASŁA
INNYM



31% 36% 

UŻYTKOWNIKÓW MEDIÓW
SPOŁECZNOŚCIOWYCH
NAWIĄZUJE KONTAKT
Z NIEZNANYMI OSOBAMI

12% UŻYTKOWNIKÓW MEDIÓW SPOŁECZNOŚCIOWYCH PRZYZNAJE, ŻE
KTOŚ WŁAMAŁ SIĘ NA ICH KONTO I PODSZYWAŁ SIĘ POD NICH

URZĄDZENIA MOBILNE I SIECI SPOŁECZNOŚCIOWE — CZYNNIKI WYWOŁUJĄCE STRES

49%

UŻYTKOWNIKÓW URZĄDZEŃ MOBILNYCH
BYŁOBY ZANIEPOKOJONYCH, GDYBY
WYSZŁO Z DOMU BEZ SWOJEGO
URZĄDZENIA MOBILNEGO



6/10

UŻYTKOWNIKÓW URZĄDZEŃ
MOBILNYCH DENERWUJE SIĘ,
GDY INNI ZAGLĄDAJĄ DO
SWOICH SMARTFONÓW I
TABLETÓW PODCZAS POSIŁKU

1/4

UŻYTKOWNIKÓW URZĄDZEŃ
MOBILNYCH ZAGLĄDA DO NICH
PODCZAS POSIŁKU Z KIMŚ
INNYM



25%

UŻYTKOWNIKÓW SIECI
SPOŁECZNOŚCIOWYCH SPRAWDZA
SWÓJ PROFIL W CIĄGU 15 MINUT
PO PRZEBUDZENIU

UŻYTKOWNICY PRZEDKŁADAJĄ WYGODĘ NAD BEZPIECZEŃSTWO

1/3

PRYZNAJE, ŻE WYGODA STAŁEGO
POŁĄCZENIA
Z INTERNETEM MA DLA NICH
WIĘKSZĄ WAGĘ NIŻ
POTENCJALNE ZAGROŻENIA

CHOCIAŻ...

40%

CHCIAŁOBY TRWALE
I CAŁKOWICIE USUNĄĆ JAKĄŚ
PRYWATNĄ TREŚĆ, KTÓRĄ
UDOSTĘPNIŁO W INTERNECIE

62%

ZGADZA SIĘ, ŻE WE
WSPÓŁCZESNYM ŚWIECIE NIE
ISTNIEJE COŚ TAKIEGO JAK
„PRYWATNOŚĆ W SIECI”

7/10

NIE ZAMIESZCZA W SIECIACH
SPOŁECZNOŚCIOWYCH ŻADNYCH
MATERIAŁÓW, KTÓRYCH NIE
POWINNI ZOBACZYĆ ICH
RODZICE/DZIECI

WNIOSKI

50% DOROSŁYCH INTERNAUTÓW
PADŁO W UBIEGŁYM ROKU OFIARĄ
CYBERPRZESTĘPCZOŚCI I/LUB NAPOTKAŁO
NEGATYWNE SYTUACJE ONLINE

PONAD MILION DOROSŁYCH PADA CODZIENNIE OFIARĄ
CYBERPRZESTĘPCZOŚCI — TO 12 OFIAR NA SEKUNDĘ

113 MLD USD

TO SUMA BEZPOŚREDNICH
KOSZTÓW CYBERPRZESTĘPCZOŚCI
NA CAŁYM ŚWIECIE W CIĄGU
ZALEDWIE 12 MIESIĘCY

**UŻYTKOWNICY PRZECHODZĄ NA URZĄDZENIA
MOBILNE, ZANIEDBUJĄ JEDNAK
BEZPIECZEŃSTWO**

KONSUMENCI W CORAZ WIĘKSZYM STOPNIU KORZYSTAJĄ Z URZĄDZEŃ
MOBILNYCH I TABLETÓW, NIE CHRONIĄ JEDNAK SAMYCH SIEBIE.
WIĘKSZOŚĆ UŻYTKOWNIKÓW ZABEZPIECZA SWOJE KOMPUTERY
STACJONARNE, DLATEGO CYBERPRZESTĘPCY ZWRÓCILI SIĘ W STRONĘ
TELEFONÓW I TABLETÓW, KTÓRE SĄ BARDZIEJ PODATNE NA ICH ATAKI.
POPULARNOŚĆ URZĄDZEŃ MOBILNYCH WCIAŻ ROŚNIE; WIDAĆ TU
PEWNE UZALEŻNIENIE OD SPRZĘTU TEGO TYPU, CO ZWIĘKSZA SZANSE
CYBERPRZESTĘPCÓW NA SKUTECZNY ATAK.

**ROZMYCIE GRANIC MIĘDZY SŁUŻBOWYM
I PRYWATNYM WYKORZYSTANIEM URZĄDZEŃ
MOBILNYCH**

PRYWATNE URZĄDZENIA MOBILNE SĄ CORAZ CZĘŚCIEJ UŻYWANE DO
WYKONYWANIA CZYNNOŚCI ZWIĄZANYCH Z PRACĄ. STYL ŻYCIA
UŻYTKOWNIKÓW STWARZA RYZYKO DLA ŚRODOWISK BIZNESOWYCH.
NIEPOKOJĄCO DUŻO FIRM NIE DYSPONUJE W TYM ZAKRESIE ŻADNĄ
POLITYKĄ. Z NASZYCH BADAŃ WYNIKA JEDNAK, ŻE NAWET W FIRMACH,
KTÓRE STWORZYŁY TAKĄ POLITYKĘ, PRACOWNICY NIE PRZESTRZEGAJĄ
JEJ ZAPISÓW.

**UŻYTKOWNICY PRZEDKŁADAJĄ WYGODĘ NAD
BEZPIECZEŃSTWO**

WIELU UŻYTKOWNIKÓW ŚWIADOMIE REZYGNUJE Z BEZPIECZEŃSTWA NA
RZECZ WYGODY; JESZCZE WIĘKSZA LICZBA NIE JEST ŚWIADOMA, ŻE TO
ROBI. „STAŁE POŁĄCZENIE Z INTERNETEM” NIE MUSI JEDNAK OZNACZAĆ
„NIEPRZERWANEGO ZAGROŻENIA”.

UWAŻAJ!

CHROŃ SWOJE DANE

WSZECHESTRONNY PAKIET ZABEZPIECZEŃ, TAKI JAK NORTON 360, ZAPEWNIĄ SOLIDNĄ OCHRONĘ PRZED ZAGROŻENIAMI W SIECI

TRAKTUJ URZĄDZENIA MOBILNE TAK SAMO JAK KOMPUTER

URZĄDZENIA MOBILNE CORAZ CZĘŚCIEJ STAJĄ SIĘ CELEM CYBERPRZESTĘPCÓW. WARTO SIĘ UPEWNIĆ, ŻE POSIADANE URZĄDZENIE JEST ZABEZPIECZONE HASŁEM I PODJĄĆ ŚRODKI OSTROŻNOŚCI, ABY ZADBAĆ O OCHRONĘ POSIADANEGO SPRZĘTU PRZED KRADZIEŻĄ, ZGUBIENIEM I CYBERPRZESTĘPCAMI

OSTROŻNIE W CHMURZE

ROZWIĄZANIA DO PRZECHOWYWANIA PLIKÓW W CHMURZE UŁATWIAJĄ ZAPISYWANIE I UDOSTĘPNIANIE INFORMACJI, STANOWIĄ JEDNAK NOWE POLE DO PRZEPROWADZANIA ATAKÓW. NALEŻY OSTROŻNIE UDOSTĘPNIĄĆ SWOJE PLIKI I W MIARĘ MOŻLIWOŚCI KORZYSTAĆ Z ROZWIĄZAŃ WYPOSAŻONYCH WE WBUDOWANE ZABEZPIECZENIA.

TRANSAKCJE POUFNE TYLKO W BEZPIECZNYCH POŁĄCZENIACH

BEZPŁATNE LUB NIEZABEZPIECZONE SIECI WI-FI MOGĄ UŁATWIĆ ZŁODZIEJOM PODSŁUCHANIE TWOICH DZIAŁAŃ. DLATEGO PODCZAS POŁĄCZENIA Z TAKIMI SIECIAMI NALEŻY UNIKAĆ PRZEPROWADZANIA JAKICHKOLWIEK POUFNYCH TRANSAKCJI, TAKICH JAK TRANSAKCJE BANKOWE CZY ZAKUPY INTERNETOWE; EWENTUALNIE MOŻNA ZASTOSOWAĆ OSOBISTEGO KLIENTA VPN.

REGULARNIE SPRAWDZAJ

WYCIĄGI Z KART KREDYTOWYCH I KONT BANKOWYCH NALEŻY SYSTEMATYCZNIE SPRAWDZAĆ POD KĄTEM EWENTUALNYCH NIELEGALNYCH TRANSAKCJI ORAZ ZGŁASZAĆ WSZELKIE PODEJRZANE DZIAŁANIA DOSTAWCY USŁUG I/LUB ODPOWIEDNIM ORGANOM.



go.symantec.com/norton-report-2013



**DZIĘKUJEMY
ZA UWAGĘ**



DALSZE WNIOSKI

POTENCJALNIE RYZYKOWNE ZACHOWANIA W NIEZABEZPIECZONYCH SIECIACH WI-FI




56% WCHODZI NA
SWOJE KONTA W SIECIACH
SPOŁECZNOŚCIOWYCH

44% 

29% WCHODZI
NA SWOJE KONTA
BANKOWE

27% 

54% KORZYSTA Z
PRYWATNYCH SKRZYNEK
POCZTOWYCH

34% 

29% ROBI ZAKUPY
ONLINE

28% 



3/10 NIE ZAWSZE
WYLOGOWUJE SIĘ PO
UŻYWANIU PUBLICZNEGO
POŁĄCZENIA WI-FI

39% NIE STOSUJE
ŻADNYCH SPECJALNYCH
ZABEZPIECZEŃ PODCZAS
KORZYSTANIA
Z PUBLICZNEJ SIECI WI-FI

ROZMYCIE GRANIC MIĘDZY PRZYJACIÓŁMI I WROGAMI

1/10 ANKIETOWANYCH WESZŁO NA KONTO
PARTNERA/PRZYJACIELA BEZ JEGO ZGODY

41%

ZROBIŁO TO
Z CIEKAWOŚCI*

26%

ZROBIŁO TO W RAMACH
WYGŁUPIANIA SIĘ/KAWAŁU*

18%

ZROBIŁO TO, BO NIE UFA
SWOJEMU PARTNEROWI/
PRZYJACIELOWI*

*WSRÓD UŻYTKOWNIKÓW, KTÓRZY WESZLI NA KONTO POCZTOWE/PROFIL
W SERWISIE SPOŁECZNOŚCIOWYM SWOJEGO PARTNERA/PRZYJACIELA

A world map composed of a grid of small dots, with the word 'METODOLOGIA' overlaid in the center.

METODOLOGIA

OPIS METODOLOGII

FIRMA EDELMAN BERLAND PRZEPROWADZIŁA BADANIE METODĄ ANKIET ONLINE. RESPONDENCI:

13022 OSOBY DOROSŁE W WIEKU OD 18 DO 64 LAT

Badanie wykonano w 24 krajach (Arabia Saudyjska, Australia, Brazylia, Chiny, Dania, Francja, Holandia, Indie, Japonia, Kanada, Kolumbia, Meksyk, Niemcy, Nowa Zelandia, Polska, Rosja, RPA, Stany Zjednoczone, Singapur, Szwecja, Turcja, Wielka Brytania, Włochy i Zjednoczone Emiraty Arabskie).

Badanie przeprowadzono w głównym języku danego kraju. Zadawane pytania były identyczne w przypadku wszystkich krajów.

Ankiety zbierano od 4 lipca do 1 sierpnia 2013 r.

Margines błędu dla całej próby dorosłych (n = 13022) wynosi 0,9% przy poziomie ufności 95%.

Ważne uwagi:

Raport „Norton Cybercrime Report” to doroczne badanie przeprowadzane na zlecenie firmy Symantec (będącej właścicielem marki Norton). Celem badania jest przeanalizowanie, jak cyberprzestępczość oddziałuje na konsumentów i w jaki sposób nowe technologie wpływają na ich bezpieczeństwo. Badanie zostało przeprowadzone przez międzynarodową firmę badawczą Edelman Berland. Wyniki opierają się na informacjach udzielonych przez ponad 13000 dorosłych użytkowników z 24 krajów.

W Stanach Zjednoczonych i Indiach ankietowano po 1000 osób dorosłych. Dane z różnych krajów zostały opatrzone wagami, tak aby wszystkie kraje były reprezentowane równo po 500 osób dorosłych.

Informacje dodatkowe:

Rynki rozwinięte: Stany Zjednoczone, Kanada, Wielka Brytania, Francja, Niemcy, Włochy, Szwecja, Holandia, Australia, Japonia, Singapur, Nowa Zelandia, Dania
Rynki wschodzące: Brazylia, Meksyk, Polska, Indie, Chiny, Rosja, Turcja, Arabia Saudyjska, ZEA, Kolumbia, RPA

Pokolenie Y: w wieku od 18 do 34 lat

Pokolenie wyżu po II wojnie światowej: w wieku od 45 do 64 lat

DEFINICJA CYBERPRZESTĘPCZOŚCI

Cyberprzestępczość definiuje się jako jedno z następujących działań:

- Wirusy komputerowe lub szkodliwe oprogramowanie na komputerze użytkownika
- Odpowiedź na podrobione, spreparowane lub sfałszowane wiadomości e-mail lub strony internetowe udające rzeczywiste próśby o odczytanie lub dostarczenie informacji do legalnego podmiotu, np. banku, i próbujące przechwycić prywatne dane użytkownika, takie jak hasła, numery kart kredytowych lub informacje o koncie bankowym
- Włamanie do skrzynki e-mail i podszywanie się pod jej właściciela
- Włamanie do profilu w serwisie społecznościowym i podszywanie się pod jego właściciela
- Odpowiedź na oszustwo internetowe
- Kradzież danych karty kredytowej w Internecie
- Kradzież tożsamości
- Wirusy na telefonach komórkowych, powodujące wysyłanie z urządzenia płatnych wiadomości tekstowych bez zezwolenia lub wiedzy użytkownika
- Zablockowanie ekranu i wyświetlenie ostrzeżenia nakazującego uiszczenie opłaty w celu odblokowania urządzenia
- Zagubienie lub kradzież smartfona albo używanie go przez jego znalazcę bez zgody właściciela
- Pojawienie się na smartfonie aplikacji, której użytkownik nie pobierał
- Podszywanie się pod przedstawiciela firmy komputerowej i informowanie użytkownika o zainfekowaniu komputera
- Inny typ cyberprzestępczości dotyczącej telefonu komórkowego lub tabletu
- Inny typ cyberprzestępczości dotyczącej komputera stacjonarnego lub laptopa

DEFINICJA CYBERPRZESTĘPCZOŚCI

Cyberprzestępczość i/lub negatywne doświadczenia online definiuje się jako jedno z następujących działań:

- Wirusy komputerowe lub szkodliwe oprogramowanie na komputerze użytkownika
- Odpowiedź na podrobione, spreparowane lub sfałszowane wiadomości e-mail lub strony internetowe udające rzeczywiste próśby o odczytanie lub dostarczenie informacji do legalnego podmiotu, np. banku, i próbujące przechwycić prywatne dane użytkownika, takie jak hasła, numery kart kredytowych lub informacje o koncie bankowym
- Włamanie do skrzynki e-mail i podszywanie się pod jej właściciela
- Włamanie do profilu w serwisie społecznościowym i podszywanie się pod jego właściciela
- Odpowiedź na oszustwo internetowe
- Kradzież danych karty kredytowej w internecie
- Kradzież tożsamości
- Wirusy na telefonach komórkowych, powodujące wysyłanie z urządzenia płatnych wiadomości tekstowych bez zezwolenia lub wiedzy użytkownika
- Zablockowanie ekranu i wyświetlenie ostrzeżenia nakazującego uiszczenie opłaty w celu odblokowania urządzenia
- Zagubienie lub kradzież smartfona albo używanie go przez jego znalazcę bez zgody właściciela
- Pojawienie się na smartfonie aplikacji, której użytkownik nie pobierał
- Podszywanie się pod przedstawiciela firmy komputerowej i informowanie użytkownika o zainfekowaniu komputera
- Inny typ cyberprzestępczości dotyczącej telefonu komórkowego lub tabletu
- Inny typ cyberprzestępczości dotyczącej komputera stacjonarnego lub laptopa
- Zamieszczenie w internecie prywatnych/intymnych zdjęć lub filmów użytkownika bez jego zgody
- Przesyłanie online niechcianych wiadomości o zabarwieniu seksualnym
- Zastraszanie lub stalking online, zbrodnia nienawiści lub inna forma nękania w sieci
- Otrzymywanie wiadomości SMS od nieznanymi osób z prośbą o kliknięcie podanego łącza lub wybranie nieznanego numeru w celu odebrania poczty głosowej, którą użytkownik rzekomo otrzymał
- Otrzymywanie niechcianych nagich zdjęć od nieznanymi osób
- Otrzymanie niechcianych nagich zdjęć od znanych osób

OBLICZENIA EKSTRAPOLACYJNE

1) Niemal 380 mln ofiar w 24 krajach w ciągu minionych 12 miesięcy

Liczba dorosłych internautów na kraj x % ofiar cyberprzestępców w ostatnich 12 miesiącach na kraj
= 377 943 431 (suma dla 24 krajów).

2) 12 ofiar cyberprzestępstw na sekundę / 719 na minutę / 43 144 na godzinę / ponad 1 milion dziennie — co wskazuje na niemal 378 mln osób dorosłych w ubiegłym roku w 24 krajach*

Liczba ofiar w ciągu ostatnich 12 miesięcy (jak wyżej)
 $377\,943\,431 / 365 \text{ dni w roku} / 24 \text{ godziny} / 60 \text{ minut} / 60 \text{ sekund}$.

3) Cyberprzestępczość to już przemysł — jej koszty sięgnęły w ubiegłym roku 113 mld USD w 24 krajach

Liczba ofiar w ciągu ostatnich 12 miesięcy (na kraj) x średni koszt cyberataku (na kraj w USD). Liczba podawana jako suma całkowitych kosztów we wszystkich krajach.