XIX edycja

Mistrzostwa Polski MŁODYCH EKONOMISTÓW

Formularz zgłoszeniowy

(należy wypełnić wielkimi literami)

Nazywam się:

Nazwisko:

Imię:

Mieszkam w:

Ulica:

Nr domu:

Nr mieszkania:

Miasto:

Kod pocztowy:

Województwo:

Tel. kontaktowy:

E-mail:

Szkoła, w której się uczę:

Nazwa szkoły:

Ulica i numer:

Miasto:

Kod pocztowy:

Województwo:

Tel. do szkoły:

E-mail:

Nazwisko i imię dyrektora szkoły:

Nazwisko i imię nauczyciela:

Oświadczam, że zapoznał-em/-am się z treścią regulaminu XIX edycji konkursu ekonomicznego „Mistrzostwa Polski Młodych Ekonomistów" (dostępnym m.in. na stronie www.skef.pl) i akceptuję zawarte w nim warunki.

Oświadczam, że jestem uczniem klasy VII lub VIII szkoły podstawowej.

Jako rodzic/opiekun prawny wyrażam zgodę na udział mojego dziecka/podopiecznego w konkursie „Mistrzostwa Polski Młodych Ekonomistów" oraz oświadczam, że zapoznał-em/-am się z treścią regulaminu XIX edycji konkursu ekonomicznego „Mistrzostwa Polski Młodych Ekonomistów" (dostępnym m.in. na stronie www.skef.pl) i akceptuję zawarte w nim warunki.

Data oraz podpis uczestnika konkursu

Data oraz imię i nazwisko i podpis rodzica/opiekuna prawnego

ORGANIZATOR

Stowarzyszenie Krzewienia Edukacji Finansowej

PATRONAT HONOROWY

NBP Narodowy Bank Polski

KASA KRAJOWA

PARTNERZY I SPONSORZY

ALIOR BANK FUNDACJA

FUNDACJA STEFCZYKA

SALTUS UBEZPIECZENIA

FUNDACJA WSPIERANIA UBEZPIECZEŃ WZAJEMNYCH

PATRONAT MEDIALNY

SIECI

wGospodarce.pl

wPolsce24

CZĘŚĆ A

Rozwiąż test. Wstaw znak X obok jednej prawidłowej odpowiedzi.

1. Najbezpieczniej jest używać:

- ☐ jednego hasła do wszystkich kont, aplikacji
- ☐ kilku haseł do większości kont, aplikacji
- ☐ skomplikowanych haseł, innego dla każdego konta, aplikacji

2. Gdy korzystasz z Internetu np. logując się do serwisów społecznościowych, wysyłając e-mail, używając komunikatora czy wyszukując informacji to zostawiasz:

- ☐ ślad wirtualny
- ☐ ślad cyfrowy
- ☐ ślad twardy

3. Płatności zbliżeniowe są prostą i wygodną metodą dokonywania transakcji. Wykorzystują technologię:

- ☐ FNC
- ☐ CFN
- ☐ NFC

4. Wiadomość SMS z informacją o konieczności dopłaty do kosztów przesyłki za zakupy internetowe może być fałszywa i być próbą wyłudzenia poufnych informacji, jak np. danych logowania, karty płatniczej czy używanych haseł. Taka metoda oszustwa to:

- ☐ phishing
- ☐ skimming
- ☐ sniffer

5. Złośliwe oprogramowanie, które może przybierać różne formy, jak np. trojany, robaki i inne wirusy nosi nazwę:

- ☐ software
- ☐ malware
- ☐ hardware

6. Jak sprawdzić, czy sklep internetowy istnieje i nie jest oszustwem?

- ☐ wystarczy sprawdzić tylko stronę www
- ☐ wystarczy sprawdzić, czy firma posiada funkcjonujące konto w mediach społecznościowych
- ☐ trzeba sprawdzić, czy firma ma stronę www, czy istnieje regulamin sklepu internetowego, czy widnieją dane firmy na stronie www oraz w rejestrach CEDiG lub KRS

7. Co to jest portfel elektroniczny?

- ☐ specjalny portfel na banknoty euro
- ☐ istnieje w przestrzeni wirtualnej i może służyć do płatności w sklepach internetowych oraz stacjonarnych
- ☐ specjalny portfel, którym można płacić jedynie w sklepach internetowych

8. Oszustwo, które polega na podszywaniu się pod dowolny numer telefonu to:

- ☐ spoofing
- ☐ stream
- ☐ spam

9. Co należy zrobić w przypadku utraty karty płatniczej?

- ☐ zgłosić utratę karty tylko na policji
- ☐ zastrzec kartę kontaktując się z instytucją finansową lub dzwoniąc pod ogólnopolski numer telefonu 828 828 828
- ☐ zastrzec kartę wyłącznie dzwoniąc pod numer alarmowy 112

10. Jak nazywamy typ wirusa, który może rozprzestrzeniać się za pośrednictwem zainfekowanego załącznika e-mail lub poprzez pobieranie plików? Może też ukrywać się w darmowych grach, aplikacjach, filmach.

- ☐ wirus Ateński
- ☐ wirus Trojan
- ☐ wirus Kreatywny

11. Rodzaj złośliwego oprogramowania, które najczęściej przez zaszyfrowanie uniemożliwia użytkownikowi dostęp do jego danych, a do ich przywrócenia wymaga wpłacenia okupu to:

- ☐ ransomware
- ☐ firewall
- ☐ VPN

12. Metodę uwierzytelnienia wykorzystującą np. odcisk palca, skan twarzy bądź obraz tęczówki oka nazywamy:

- ☐ cybermetrią
- ☐ biometrią
- ☐ cyfrometrią

13. Oszustwo metodą „na blik" polega na:

- ☐ wyłudzeniu 4-cyfrowego numeru PIN do dokonania płatności
- ☐ wyłudzeniu indywidualnego hasła do dokonania płatności
- ☐ wyłudzeniu 6-cyfrowego kodu do dokonania płatności

14. Bezpiecznych zakupów w Internecie nie zapewniają:

- ☐ wirtualne portfele
- ☐ płatności za pośrednictwem publicznych sieci Wi-Fi
- ☐ płatności kartami płatniczymi

15. Oprogramowanie szpiegujące, które śledzi ruch na klawiaturze i przekazuje dane osobom trzecim to:

- ☐ wirtualscreen
- ☐ tablesaver
- ☐ keylogger

16. Skimmer umieszczony w bankomacie służy do:

- ☐ bezprawnego kopiowania danych z paska magnetycznego karty płatniczej
- ☐ przedłużenia terminu ważności karty płatniczej
- ☐ identyfikacji tożsamości osoby dokonującej wypłaty w bankomacie

17. Sniffery pozwalają na:

- ☐ zwiększenie pojemności dysku
- ☐ wykrycie nieautoryzowanego przelewu
- ☐ nieautoryzowany monitoring aktywności sieci, haseł, loginów, wykradanie danych szczególnie powiązanych z dostępami do bankowości elektronicznej

18. Obecnie bezpieczne hasło składa się przynajmniej z 12 znaków (a nawet więcej), w którym powinny być użyte:

- ☐ tylko cyfry, wielkie litery i znaki specjalne
- ☐ tylko małe litery, cyfry i znaki specjalne
- ☐ małe i wielkie litery, cyfry i znaki specjalne

19. Najbezpieczniej jest, aby zawsze po zakończonej transakcji, przeczytaniu e-maili lub innej czynności na jakimkolwiek internetowym koncie:

- ☐ wylogować się
- ☐ zapisać login i hasło w przeglądarce internetowej
- ☐ tylko zamknąć komputer lub inne urządzenie, z którego korzystasz

20. Niechciane lub niepotrzebne wiadomości elektroniczne, wysyłane za pośrednictwem poczty elektronicznej, komunikatorów, a także SMS-ów to:

- ☐ scanner
- ☐ spam
- ☐ smart

21. Celem zmniejszenia ryzyka utraty danych zgromadzonych na smartfonach, tabletach i komputerach jest regularne:

- ☐ wykonywanie kopii bezpieczeństwa danych zgromadzonych na urządzeniach
- ☐ aktualizowanie bazy kontaktów
- ☐ weryfikowanie szybkości transferu danych

22. Dodatkowe zabezpieczenie, które wymaga od użytkownika podania dwóch różnych form uwierzytelnienia tożsamości przed uzyskaniem dostępu do konta lub usługi nosi nazwę:

- ☐ kontroli dwuetapowej
- ☐ uwierzytelniania dwuskładnikowego
- ☐ zabezpieczenia dwuwariantowego

23. W zarządzaniu hasłami może pomóc:

- ☐ zbiór haseł
- ☐ magazyn haseł
- ☐ menedżer haseł

24. Podejrzane wiadomości SMS można zgłaszać do CERT Polska na bezpłatny numer telefonu:

- ☐ 7070
- ☐ 8080
- ☐ 9090

25. Jakie dane można podać w wiadomości prywatnej SMS w związku z zakupem przedmiotu wystawionego na platformie ogłoszeniowej?

- ☐ jedynie informacje odnoszące się do szczegółów zamówienia, bez danych dotyczących płatności czy informacji o karcie płatniczej
- ☐ wszystkie dane, jakich żąda sprzedający
- ☐ jedynie dane dotyczące płatności, takie jak: numer karty, data jej ważności i 3-cyfrowy kod CVV lub CVC

26. Vishing to:

- ☐ nazwa programu antywirusowego
- ☐ oszustwo polegające na pozyskiwaniu danych np. numer konta, hasła dostępu do konta lub skłanianiu do wykonania pewnych działań w trakcie rozmowy telefonicznej
- ☐ aplikacja internetowa do kontroli budżetu domowego

27. Metoda oszustwa, w której wykorzystuje się kody QR to:

- ☐ qwerty
- ☐ chargeback
- ☐ quishing

28. Związek Banków Polskich był inicjatorem i prekursorem budowy systemu, który chroni przed wyłudzeniami z użyciem cudzej tożsamości. Jest to system o nazwie:

- ☐ dokumenty zastrzeżone
- ☐ dokumenty niedozwolone
- ☐ dokumenty zabezpieczone

29. Chatboty oraz wirtualni asystenci, w tym rozwiązania wykorzystujące rozpoznawanie mowy wykorzystywane w bankowości, oparte są o:

- ☐ sztuczną inteligencję
- ☐ sztuczną sieć
- ☐ sztuczny interfejs

30. Smishing to rodzaj oszustwa, które przestępcy przeprowadzają za pomocą:

- ☐ przesyłki
- ☐ SMS
- ☐ listu poleconego

CZĘŚĆ B

1. **Wymień pięć podstawowych zasad cyberhigieny:**

1.
2.
3.
4.
5.

2. **Wymień trzy cechy, które mogą wskazywać na wiadomość phishingową.**

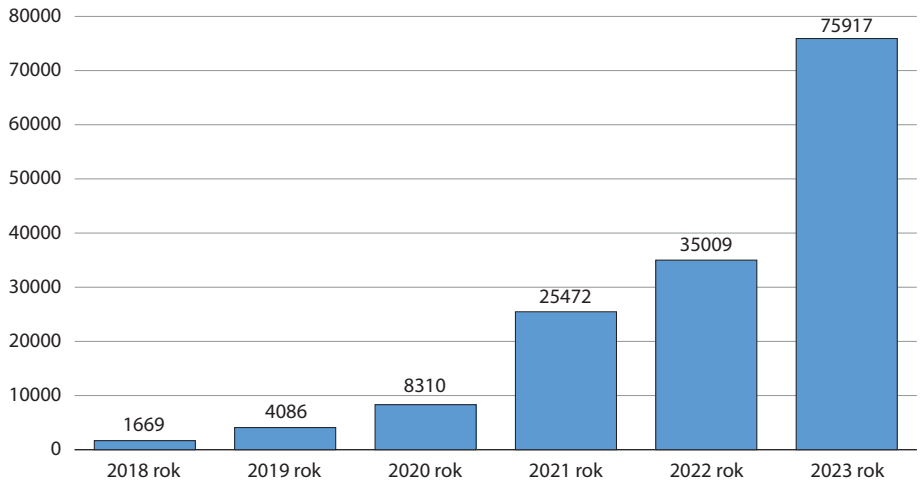
1.
2.
3.

3. **Napisz, co należy zrobić, aby zabezpieczyć się przed utratą danych osobowych, które mogą umożliwić przestępcom zaciągnięcie kredytu lub pożyczki w naszym imieniu.**

CZĘŚĆ C

Wykorzystując dane z wykresów, wykonaj obliczenia i udziel odpowiedzi na pytania 1-3.

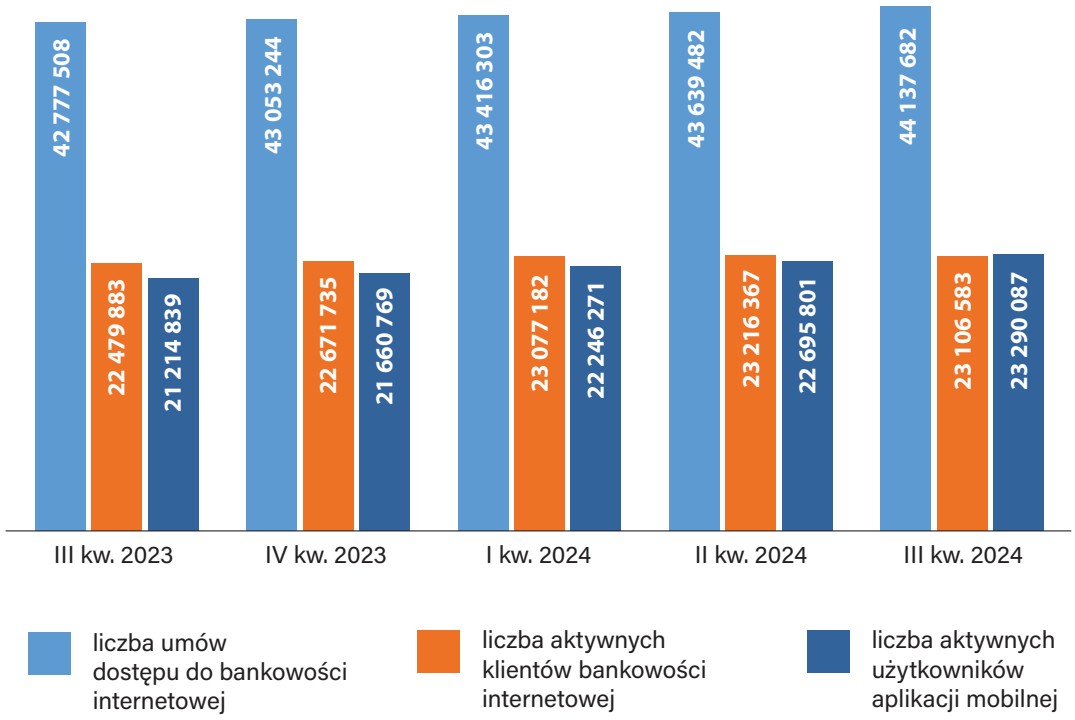
Wykres 1. Liczba oszustw komputerowych zarejestrowanych przez CERT Polska w okresie 2018-2023.



Źródło: Na podstawie danych z raportów rocznych z działalności CERT Polska 2018-2023.

1. W którym roku nastąpił największy wzrost procentowy zarejestrowanych przestępstw komputerowych w odniesieniu do roku poprzedzającego? Przedstaw obliczenia dla każdego roku od 2019 do 2023.

Wykres 2. Liczba aktywnych użytkowników aplikacji mobilnej w okresie od III kwartału 2023 do III kwartału 2024 r.



Źródło: Raport III kwartał 2024 NetB@nk bankowość internetowa i mobilna, płatności bezgotówkowe.

2. Oblicz, jaki procent użytkowników mających dostęp do bankowości internetowej w III kwartale 2024 roku aktywnie z niej korzystało.

3. **W którym kwartale 2024 roku liczba aktywnych użytkowników aplikacji mobilnej przekroczyła liczbę aktywnych użytkowników bankowości internetowej? Oblicz, o ile procent?**

4. **Przedstaw swoją opinię na temat:**
Bezpieczeństwo finansowe w codziennym życiu - jak dbać o finanse osobiste w obliczu cyberzagrożeń?