# S3 - IT Security

# Przykładowy test egzaminacyjny

# Odpowiedzi do testu

1. Czym może grozić ujawnienie wszystkich danych osobowych (łącznie ze zdjęciem) widocznych w dowodzie osobistym, tzw. kradzież tożsamości?
2. Utratą danych na dysku mojego komputera.
3. Zwiększoną liczbą spamu, czyli niechcianej poczty elektronicznej.
4. **Kłopotami np. z bankiem, w którym zaciągnięto kredyt na moje nazwisko.**
5. Udostępnienie danych osobowych nie stanowi zagrożenia w skomputeryzowanym świecie.
6. Które z widocznych poniżej prób wyłudzenia informacji są prawdziwe?
7. **Pretexting** polega na tym, że przestępca dzwoni do konsumenta starając się pozyskać przez telefon dane umożliwiające uzyskanie dostępu do rachunku bankowego ofiary.
8. ***Vishing*** oznacza przestępstwa polegające na wyłudzeniu poufnych informacji z wykorzystaniem technologii VoIP (voice over Internet Protocol technology).
9. ***Pharming***- metoda oszustwa, bardziej niebezpieczna oraz trudniejsza do wykrycia forma ***phishingu***. Po wpisaniu prawidłowego adresu strony, zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę WWW.
10. **Wszystkie odpowiedzi są poprawne.**
11. Które z poniższych działań użytkownika komputera **nie** stanowi zagrożenia dla bezpieczeństwa danych?
12. Częste wykonywanie kopii zapasowej systemu operacyjnego.
13. Częste archiwizowanie szyfrowanych plików na zewnętrznym nośniku danych.
14. Zabezpieczanie przed otwarciem ważnych dla użytkownika plików hasłem.
15. **Wszystkie odpowiedzi są poprawne.**
16. Który z poniższych programów powinien być instalowany możliwie szybko, po instalacji systemu operacyjnego?
17. Przeglądarka internetowa, niebędąca składnikiem systemu operacyjnego.
18. Aplikacje umożliwiające dostęp do portali społecznościowych.
19. **Program antywirusowy.**
20. Program do obsługi kont pocztowych.
21. W jakich regionach świata może być wykorzystywane urządzenie elektryczne z tabliczką znamionową:
	1. **We wszystkich regionach świata.**
	2. Tylko na terenie Europy.
	3. Tylko na terenie Azji.
	4. Tylko na terenach obu Ameryk.
22. Które z poniższych stwierdzeń prawidłowo opisuje sieć komputerową LAN?
23. Autoryzowana sieć dostępu do poufnych danych (ang. Legally Area Network).
24. **Sieć lokalna (ang. Local Area Network) – łącząca komputery na określonym obszarze takim jak budynek mieszkalny, szkoła, uczelnia lub biuro.**
25. Wszystkie sieci (ang. Locomotor Area Network) – łączące przenośne komputery i urządzenia z nimi współpracujące.
26. Żadna z tych odpowiedzi nie jest poprawna.
27. Pracując w sieci komputerowej należy zwracać szczególną uwagę na:
28. Korzystanie z protokołu https przy przesyłaniu wrażliwych danych.
29. Zachowanie w maksymalnym stopniu swojej prywatności, czyli niepublikowaniu numeru telefonu, adresu lub numeru PESEL na portalach społecznościowych.
30. Aktualizację programu antywirusowego i wszelkich innych, wykorzystywanych podczas pracy w sieci.
31. **Wszystkie odpowiedzi są poprawne.**
32. Dlaczego należy chronić dane osobowe przechowywane na firmowym serwerze?
33. Aby zapobiec wycieku poufnych informacji.
34. Aby nie dopuścić do sfałszowania lub usunięcia danych.
35. Aby być w zgodzie z obowiązującym prawem.
36. **Wszystkie odpowiedzi są poprawne**.
37. Dane nie mogą być zmienione bez naruszenia:
38. Poufności danych.
39. Właściwości, czyli zmiany atrybutów pliku.
40. Rozmiaru pliku.
41. **Integralności danych.**
42. Jaki rodzaj oprogramowania gromadzi informacje o aktywności użytkowników w sieci bez ich wiedzy i zgody?
43. Przeglądarki internetowe zapisując dane w małych plikach tekstowych, tzw. cookies.
44. Oprogramowanie szpiegujące (ang. malware).
45. **Oprogramowanie szpiegujące (ang. spyware).**
46. Funkcja Historia przeglądarki internetowej.
47. Początek formularza
48. Przyczyną nadmiernej liczby niechcianych przesyłek (spamu) może być:
49. Duża liczba kontaktów wpisanych w książce adresowej.
50. Brak, lub zbyt proste hasło zabezpieczające skrzynkę pocztową.
51. **Brak filtru poczty elektronicznej lub zawirusowany komputer.**
52. Błędny wpisany w programie pocztowym adresu poczty elektronicznej.
53. Dół formularza
54. Podczas korzystania z serwisów społecznościowych użytkownicy narażeni są na:
55. ***Phishing*** - otrzymywanie wiadomości z próbą wyłudzenia poufnych informacji.
56. ***Shoulder surfing***- spoglądanie przez ramię ofiary w celu pozyskania poufnych danych.
57. ***Grooming* - nawiązanie relacji między osobami dorosłymi a dziećmi w celu ich uwiedzenia i wykorzystania seksualnego.**
58. ***Pretexting*** - praktyki pozyskiwania danych osobowych pod fałszywym pretekstem, nieprawidłową czynność, która prowadzi do kradzieży tożsamości.
59. W odebranej przesyłce poczty elektronicznej znajdują się pliki wykonywalne i plik arkusza kalkulacyjnego z informacją:

1. **Otwarcie załącznika i włączenie edytowania może doprowadzić do zainfekowania komputera.**
2. Otwarcie załącznika może doprowadzić do zainfekowania komputera, włączenie edytowania nie spowoduje nigdy zagrożenia.
3. Otwarcie załącznika nie spowoduje nigdy zagrożenia, włączenie edytowania może doprowadzić do zainfekowania komputera.
4. Otwarcie załącznika i włączenie edytowania nie spowoduje nigdy zagrożenia infekcją komputera.
5. E-mail o treści przedstawionej poniżej jest:

Drodzy Substribers webmail.

Ze względu na bieżące utrzymanie na naszym serwerze,

W pierwszym kwartale 2017 roku, aby utrzymać swoje konto e-mail, bezpieczne od spamerów, Niedawno wykryto nietypowe działania z konta e-mail, wiec skrzynka pocztowa została tymczasowo zawieszona przez Admin.

Należy odzyskać swoje konto, klikając na poniższy link lub skopiuj do przeglądarki:

Kliknij Tutaj

Przepraszamy za niedogodności.
System pomocy administracyjne

1. ***Ransomware*** – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji.
2. ***Phishing*** **- metoda oszustwa, próba wyłudzenia loginu i hasła konta pocztowego.**
3. ***Fraudulent*** - oszukańczy e-mail wprowadzający w błąd odbiorcę poczty elektronicznej.
4. Informacją o rzeczywistej awarii serwisu pocztowego.
5. Jaką czynność należy wykonać, aby wiadomość e-mail została odczytana tylko przez właściwe osoby?
6. **Zaszyfrować wiadomość kluczem publicznym i odszyfrować kluczem prywatnym.**
7. Podpisać cyfrowo wysyłaną wiadomość.
8. Podpisać cyfrowo wiadomość i każdy znajdujący się w nim załącznik.
9. Nie ma potrzeby dodatkowych zabezpieczeń, bo poczta elektroniczna jest bezpiecznym sposobem przesyłania informacji.
10. Aby ograniczyć maksymalnie straty energii elektrycznej po naładowaniu baterii lub akumulatora urządzenia mobilnego należy:
11. Odłączyć kabel zasilający od urządzenia, pozostawiając ładowarkę połączoną z siecią energetyczną.
12. Nie ma konieczności rozłączania urządzeń, ponieważ pobór energii elektrycznej w czasie ładowania i po jego zakończeniu jest tak mały, że liczniki nie rejestrują ich poboru.
13. Nie ma konieczności rozłączania urządzeń, ponieważ po naładowaniu ogniw system odcina pobór prądu elektrycznego.
14. **Odłączyć kabel zasilający od urządzenia i ładowarkę od sieci energetycznej.**
15. **Firewall** – (ściana przeciwogniowa) to:
16. Część systemu operacyjnego zapewniająca integralność plików systemowych.
17. **Jeden ze sposobów zabezpieczania sieci komputerowych i systemów operacyjnych przed intruzami.**
18. Rozbudowany, elektroniczny system ochrony przeciwpożarowej w nowym budownictwie.
19. Składnik systemu operacyjnego zabezpieczający przed nadmiernym wzrostem temperatury wewnątrz komputera.
20. Które ze zdań prawdziwie charakteryzuje **firewall**?
21. Poprawnie skonfigurowany firewall odeprze wszelkie typy ataków na nasz komputer.
22. **Firewall nie zawsze powstrzyma ataki i nie poinformuje użytkownika o nieautoryzowanym wtargnięciu do komputera.**
23. Firewall  jest zaporą sieciową, zapewniającą darmową, kompleksową ochronę tylko dla użytku prywatnego lub niewielkich firm.
24. Firewall  jest zaporą sieciową, zapewniającą darmową, kompleksową ochronę tylko dla użytku komercyjnego.
25. Aby zapewnić poufność danych znajdujących się w urządzeniu, przy pomocy którego korzystamy z portali społecznościowych należy:
26. **Maksymalnie ograniczyć dostępność plików.**
27. Aktualizować często program antywirusowy.
28. Szyfrować przesyłane informacje.
29. Nie korzystać z otwartych punktów dostępu, tzw. hotspotów.
30. Które z poniższych haseł najlepiej zabezpiecza przed nieautoryzowanym dostępem do konta poczty elektronicznej?
31. 123456
32. **amCm\_w>12%**
33. 12.03.2017 - data urodzin członka rodziny.
34. Mariola - imię członka rodziny.
35. VoIP (ang. voice over internet protocol) to technika umożliwiająca przesyłanie dźwięków za pomocą łączy internetowych wykorzystujących protokół IP, popularnie nazywana „telefonią internetową”.
Luką bezpieczeństwa w tym protokole może być:
36. Niewłaściwa konfiguracja programu VoIP.
37. **Backdoor (pol. tylne drzwi, furtka) – luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania.**
38. "Podsłuchiwanie" rozmów przez inne osoby zalogowane do tej samej sieci komputerowej.
39. Zainstalowany w komputerze program typu spyware (oprogramowanie szpiegujące).
40. Instalowanie w smartfonie lub tablecie gier pobieranych np. z App Store może spowodować:
41. Zwiększenie szybkości pracy urządzenia mobilnego.
42. Zwiększenie bezpieczeństwa danych przechowywanych w urządzeniu mobilnym.
43. **"Wyciek" prywatnych informacji z naszego urządzenia.**
44. Zwiększenie szybkości transferu danych w sieci Wi-Fi.
45. Co może zapewnić poprawę bezpieczeństwa sprzętu komputerowego i znajdujących się w nim informacji?
46. **Kontrola dostępu do sprzętu i danych w nim znajdujących się.**
47. Częsta aktualizacja programu antywirusowego.
48. Instalacja i częsta aktualizacja przynajmniej dwóch programów antywirusowych.
49. Aktualizacja systemu operacyjnego.

## KopiaWskaż prawidłową odpowiedź:

Początek formularza

Spoglądając na powyższy obraz, możesz sądzić, że:

1. Wykonanie kopii zapasowej systemu na tym nośniku jest mało prawdopodobne z powodu zbyt małej przestrzeni na wybranym nośniku danych.
2. Wykonanie kopii zapasowej systemu w tej konfiguracji jest możliwe poprzez zapisanie jej w
3. Wykonanie kopii zapasowej systemu w tej konfiguracji jest możliwe po zwiększeniu wolnej przestrzeni na dysku G.
4. **Wszystkie odpowiedzi są poprawne.**
5. Hotspot (ang. hot spot – „gorący punkt”) to:
6. Miejsce w komputerze o najwyższej temperaturze.
7. Funkcja lub aplikacja w smartfonach umożliwiająca dostęp do Internetu.
8. Funkcja lub aplikacja w smartfonach informująca o nadmiernym wzroście temperatury urządzenia.
9. **Otwarty punkt dostępu, umożliwiający połączenie z Internetem, za pomocą sieci bezprzewodowej opartej na standardzie Wi-Fi.**

Jeżeli osiągnąłeś/aś 76% dobrych odpowiedzi czyli 19 z 25 i zrobiłeś/aś zadanie w czasie 45 minut to masz szanse zdać pozytywnie egzamin z ECDL S3

Dół formularza