IT biztonsági kérdések (helyes válaszokkal)

1. Melyik tevékenység kiberbűnözés?
   a) bedarálás
   b) adathalászat
   c) etikus hackelés
   d) titkosítás
2. Mit jelent a "hackelés" fogalma?
   a) az adatokhoz való jogosulatlan hozzáférés megszerzése
   b) félrevezetni a személyazonosságunkról valakit az interneten
   c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
   d) számítógépeket lopni az épületbe való betöréssel
3. Melyik jelent „vis maior" fenyegetést az adatokra?
   a) emberi tevékenység
   b) adatlopás
   c) tűz
   d) vírusok
4. Mi a személyes adatok védelmének célja?
   a) az etikus hackelés megelőzése
   b) a személyazonosság-lopás megakadályozása
   c) helyet lehessen megtakarítani a számítógép háttértárolóján
   d) a számítógépes vírusok elkerülése
5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
   a) bizalmasság
   b) sértetlenség
   c) rendelkezésre állás
   d) hitelesség
6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
   a) csak az informatikusokra vonatkoznak
   b) csak a pénzügyi intézmények számára fontosak
   c) csak olvasni kell, de nem kell megvalósítani
   d) fontosak, mivel követendő szabályokat adnak a felhasználók számára.
7. Melyik NEM közvetlen következménye a szélhámosságnak?
   a) a személyes adatok mások által hozzáférhetővé váltak
   b) hozzáférhetővé vált mások által a számítógép-rendszer
   c) a tűzfalat kikapcsolják
   d) a begyűjtött adatokat csalásra fogják felhasználni
8. Melyik a személyazonosság-lopás módszere?
   a) hamis név használata egy közösségi oldalon
   b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
   c) adatok elektromágneses eszközökkel történő megsemmisítése
   d) információbúvárkodás
9. Mi használható egy rosszindulatú program elrejtésére?
   a) kikérdezés
   b) rendszerszinten tevékenykedő kártékony kód

c) biometria
d) bankkártya-lemásolás

10. Mit lehet adatlopásra használni?
a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

11. Mi a vírusirtó szoftverek korlátja?
a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

12. Mi igaz a karanténban lévő fájlokra?
a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

13. Mi a célja a szoftverfrissítések telepítésének?
a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

14. Melyik írja le a LAN-t?
a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

15. Mi a tűzfal feladata?
a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

16. Melyik ikon jelenti a drótnélküli hálózatot?

a) 

b) 

c) 

d) 

17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?
    a) nem lehet hozzáférni a privát hálózathoz
    b) megfertőződhet a számítógép rosszindulatú szoftverekkel
    c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
    d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik
18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?
    a) megelőzi a hálózathoz való csatlakozási késedelmet
    b) biztosítja a vírusirtó szoftver naprakészségét
    c) így csak jogos felhasználó használhatja a hálózatot
    d) megvédi a hálózati tűzfalat
19. Melyik biometriai védelem?
    a) adatok mentése
    b) bankkártya lemásolása
    c) kikérdezés
    d) retina-szkennelés
20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?
    a) a web-oldal biztonságához
    b) az automatikus kiterjesztés bekapcsolásához
    c) a Lomtárnak a tranzakciót követő kiürítéséhez
    d) a tranzakciót követő elektromágneses törléshez
21. Melyik ikon jelzi a biztonságos web-oldalt?
    a) 
    b) 
    c) 
    d) 
22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
    a) crackelés
    b) eltérítéses adathalászat
    c) etikus hackelés
    d) információ-szerzés
23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
    a) tűzfal
    b) trójai program
    c) rendszerszinten rejtőző kártékony kód
    d) süti
24. Mitől kell tartanunk a közösségi média használatakor?
    a) biometria
    b) etikus hackelés
    c) internetes zaklatás
    d) titkosított fájlok

25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
    a) az elektronikus levél aláírással való ellátása
    b) ***az elektronikus levél titkosítása***
    c) egyszerű szöveges elektronikus levél formázása
    d) definíciós fájl hozzáadása az elektronikus levélhez
26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
    a) adathalászat
    b) kifigyelés
    c) billentyűzet-leütés naplózás
    d) zombi-hálózati szoftver
27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
    a) elektronikus levél
    b) fájl-megosztás
    c) eltérítéses adathalászat
    d) azonnali üzenetküldés
28. Mi használható az eszközök fizikai biztonságának növelésére?
    a) vírusirtó szoftver
    b) titkosított szöveges dokumentumok
    c) biztonsági kábel
    d) elektromagnetikus törlés
29. Melyik módszer törli visszaállíthatatlanul az adatokat?
    a) jelszavas tömörítés alkalmazása
    b) az adatokat tartalmazó lemez bedarálása
    c) a fájlok Lomtárba mozgatása
    d) adatok titkosított merevlemezre való elhelyezése
30. Mi a “jelszó crackelés” jelentése?
    a) személyes adatokat lopni on-line módon
    b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
    c) nem megfelelő jelszavak egymás utáni bevitele
    d) a jelszó nyílt szöveges verziójának megszerzése
31. Mi jelent fenyegetést az adatokra?
    a) titkosítás
    b) emberi tevékenység
    c) biometria
    d) sütik
32. Mi az üzletileg érzékeny információk védelmének célja?
    a) biztosítani a makrók engedélyezését
    b) megakadályozni a vírusok terjedését
    c) megelőzni az ügyfelek adataival való visszaélést
    d) megakadályozni az internetes zaklatás előfordulását
33. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
    a) a fájlok tömörítése
    b) internet-szűrő alkalmazása
    c) adatmentés készítése
    d) jelszóhasználat
34. Melyik az európai adatvédelmi szabályozás?
    a) ***1995 Európai Adatvédelmi Irányelv***
    b) 2001 Információs Társadalom Irányelv
    c) 1995 Európai Adat Információ Szabályzat

d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz

35. Melyik a személyazonosság-lopás leírása?
    a) felhasználói név használata az interneten
    b) felvenni más személy azonosságát haszonszerzés céljából
    c) munkahelyi adatok megadása internetes vásárláskor
    d) tartalomellenőrző szoftverek használata internetezés közben
36. Mi a makrók tiltásának hatása
    a) a makró nem fog futni
    b) a makró törölve lesz a fájlból
    c) a makró még mindig helyesen fog futni
    d) a makró akkor fog működni, ha a tűzfal be van kapcsolva
37. Mi a titkosított adatok előnye?
    a) nem lehet törölni
    b) gyorsabban lehet menteni
    c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
    d) kulcs nélkül nem lehet elolvasni
 8. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?
    a) tűzfal
    b) tartalomellenőrző szoftver
    c) rosszindulatú programkód
    d) vírusirtó szoftver és vírusdefiníciós fájlok
39. Mi vezethet rosszindulatú programkódok telepítéséhez?
    a) a makrók letiltása az alkalmazásokban
    b) hátsó kapu használata a rendszerbiztonság megkerüléséhe
    c) a “vis maior” esetekre való hivatkozás
    d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához
40. Melyik egy fertőző rosszindulatú szoftver?
    a) a féreg
    b) a süti
    c) a tűzfal
    d) a digitális tanúsítvány
41. Melyik igaz a rosszindulatú programkódokra?
    a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
    b) billentyűzet-leütés naplózását a billentyű lenyomásával lehet engedélyezni a számítógépen
    c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
    d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten
42. Hogyan működnek a vírusirtó szoftverek?
    a) fertőzésmentesített fájlokat helyeznek a karanténba
    b) észlelik a vírusokat, de nem törlik automatikusan őket
    c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
    d) ütemezett keresést használnak a vírusok észlelésére
 3. Mi a virtuális magánhálózat (VPN)?
    a) nem kell jelszó a hálózati csatlakozáshoz
    b) megengedi bárki csatlakozását egy magánhálózathoz
    c) biztonságos saját hozzáférést biztosít a hálózathoz
    d) kis földrajzi területen több összekötött számítógép együttese

44. Mi a tűzfal korlátja?
    a) fertőzött fájlokat helyez a karanténba
    b) nem értesít automatikusan a hálózati behatoláskor
    c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
    d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére
45. Mi a WPA
    a) Wired Protected Access
    b) Wi-Fi Protected Access
    c) Wired Prevention Access
    d) Wi-Fi Password Access.
46. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?
    a) a hálózati tűzfalat ki kell kapcsolni
    b) a sütiket frissíteni kell
    c) az adatokhoz hozzá akarnak férni mások
    d) az egyszer használatos jelszó ki lesz kapcsolva
47. Melyik a védett drótnélküli hálózat ikonja?
    a) 
    b) 
    c) 
    d) 

48. Melyik számít jó jelszónak?
    a) jBloggs_12091980
    b) 12092010
    c) jb
    d) jenniferBloggs
49. Mi azonosítja a biztonságos web-oldalakat?
    a) .org
    b) .com
    c) https
    d) htt
50. Mit jelent az eltérítéses adathalászat (pharming)?
    a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
    b) a webforgalom átirányítása egy hamisított web-oldalra
    c) a kifigyelés egyik módszere
    d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése
51. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
    a) automatikus kiegészítés

b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

52. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

53. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

4. Mit nem szabad közzétenni egy közösségi oldalon?
a) zenei érdeklődésta
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

55. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
a) jelszavas tömörített fájl
b) digitális aláírás
c) makró
d) makrózott titkosított szöveg

56. Mi az adathalászat?
a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

57. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?
a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

58. Mi az azonnali üzenetküldés sebezhetősége?
a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior
d) információbúvárkodás

59. Mi jelenti az adatok végleges megsemmisítését?
a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

60. Mi az információ információbiztonsági szempontból?
a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

61. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

62. Mi NEM fenyegeti az adatokat?
a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

63. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

64. Mi a szélhámosság közvetlen következménye?
a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

65. Mi a kikérdezés?
a) szöveges üzenetküldés a telefonszolgáltató weboldaláról
b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

66. Mi a titkosítás korlátja?
a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

67. Mi a rosszindulatú programkód?
a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

68. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?
a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

69. Mi az előnye a vírusirtóknak?
a) megakadályozzák a kifinomult támadásokat
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

70. Miért kell vírusdefiníciós fájlokat letölteni?
a) frissíti az ideiglenesen letöltött és tárolt fájlokat

b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

71. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?
a) LAN
b) VPN
c) WAN
d) USB

72. Mi a hálózati adminisztrátor feladata?
a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

73. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?
a) elektromágneses törlés
b) tűzfalak
c) adathalászat
d) digitális tanúsítványok

74. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?
a) 
b) 
c) 
d) 

75. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?
a) adatok biztonsági mentése
b) fájlok tömörítése
c) személyes adatok védelme
d) információbúvárkodás

76. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?
a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

77. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?
a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

78. Mikor használnak egyszer használatos jelszót?
a) a laptopra való első bejelentkezéskor
b) amikor a jelszót elküldik e-mailben

c) amikor tűzfalat állítanak be
d) VPN-be való bejelentkezéskor

79. Melyik adat törölhető a böngésző által?
a) kititkosított adat
b) titkosított adat
c) automatikus kiegészítés adata
d) billentyűzet-leütéseket naplózó adat

80. Melyikkel korlátozható az interneten töltött időtartam?
a) adathalász szoftver
b) szülői felügyelet szoftver
c) tárcsázó
d) sütik

81. Melyik a közösségi oldalakon előforduló fenyegetés?
a) bedarálás
b) elektromágneses törlés
c) bankkártya adatainak a lemásolása
d) szexuális kizsákmányolás

82. Milyen eljárás biztosítja az e-mailek bizalmasságát?
a) titkosítás
b) kikérdezés
c) eltérítéses adathalászat
d) kititkosítás

83. Mi a digitális aláírás eszköze?
a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
b) egy matematikai séma az üzenet hitelességének biztosítására
c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására

84. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?
a) kifigyelés
b) internetes zaklatás
c) adathalászat
d) crackelés

85. Mi tartalmazhat rosszindulatú programkódot?
a) levélcsatolmány
b) süti
c) tűzfal
d) digitális aláírás

86. Melyik nyújt védelmet az adatvesztés ellen?
a) sütik
b) kikérdezés
c) titkosított USB lemez használata
d) mentések

87. Miért van szükség az adatok visszaállíthatatlan törlésére?
a) az áramingadozásból adódó meghibásodások miatt
b) az adatok más általi visszaállíthatatlansága miatt
c) hogy tartalomellenőrző szoftvert lehessen telepíteni
d) hogy törölni lehessen minden sütit

88. Melyik kiberbűnözés az alábbiak közül?
a) okostelefon ellopása
b) internetes számla on-line befizetése
c) bankkártya adatok ellopása on-line
d) internetes rádióhallgatása on-line

89. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

a) crackelés
b) etikus hackelés
c) bankkártya adatainak lemásolása
d) kikérdezés

90. Miért kell védeni az üzletileg érzékeny információkat?
a) mert megakadályozza az adatlopást
b) ütemezett mentések lefutásának biztosítása miatt
c) kéretlen üzenetek blokkolása miatt
d) a biztonságos weboldalak azonosításáért

91. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
a) bonyolult fájlnevek
b) billentyűzet-leütés naplózása
c) eltérítéses adathalászat
d) titkosítás

92. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

93. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában??
a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 1995 Európai Adatvédelmi Irányelv
d) 2001 Európai Irányelv az Információ-Technológiáról

94. Melyik tartozik a szélhámosság módszerei közé?
a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

95. Mi a személyazonosság-lopás közvetlen következménye?
a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

96. Melyik szoftvert készítik és küldik károkozási célból?
a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

97. Mit használnak a rosszindulatú programkódok elrejtésére?
a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

98. Mi egy fertőző, rosszindulatú program?
a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

99. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?
a) biometria
b) vírus-definíciós fájl
c) süti

d) zombi-hálózat

100. Mi a vírusirtó szoftverek előnye?
a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

101. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?
a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program
c) zombi-hálózati szoftver
d) tűzfalak

102. Mi biztosítja a vezeték nélküli biztonságot?
a) WAN
b) LAN
c) Média Hozzáférési Kontroll (MAC)
d) számítógépes hálózathoz hátsó kaput nyitó szoftver

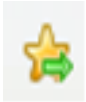
103. Mi eredményezhet jogosulatlan adathozzáférést??
a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

104. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?
a) 
b) 
c) 
d) 

105. Hogyan történik a hálózati bejelentkezés?
a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

106. Melyik a jó szabály a jelszavakra?
a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

107. Melyik weboldalnál található http előtag a https helyett?
a) on-line bank
b) keresőmotor
c) on-line webáruház
d) biztonságos weboldal

108. Melyik jelöli a biztonságos weboldalakat?
a) 

b) 

c) 

d) 

109. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
    a) vírusdefiníciós fájlok
    b) titkosított adatbázis-mentési fájlok
    c) makrók
    d) digitális tanúsítványok
110. Miért kell a sütiket blokkolni a böngészőkben?
    a) hogy vírusirtó szoftvert lehessen telepíteni
    b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
    c) hogy böngészhessünk ismeretlen weblapokon
    d) hogy megakadályozzuk az internetes zaklatást
111. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
    a) a személyes adatokhoz csak a barátok férhetnének hozzá
    b) a személyes adatokat bárki megnézheti
    c) a barátok barátai láthatnák a személyes adatokat
    d) a barátok módosíthatnák a személyes adatokat
112. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
    a) X509v3 digitális tanúsítványok
    b) tűzfalak
    c) digitális aláírások
    d) csalárd elektronikus levelek
113. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
    a) rendszerszinten tevékenykedő kártékony kódok
    b) tárcsázó programok
    c) adathalászat
    d) bankkártya-lemásolás
114. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
    a) rosszindulatú programkódokat tartalmazhat
    b) lehet, hogy nagyon nagy a fájl
    c) lehet, hogy titkosító kulcs szükséges a megnyitásához
    d) lehetséges, hogy digitális tanúsítványt tartalmaz
115. Melyik lehet az azonnali üzenetküldés sebezhetősége?
    a) vírusdefiníciós fájlok
    b) on-line emelt díjas tárcsázó programok
    c) digitális tanúsítványok
    d) rosszindulatú programkódok
116. Melyik egy lehetséges mentési tulajdonság?
    a) bankkártya lemásolás
    b) ütemezés
    c) kikérdezés
    d) elektromágneses törlés
117. Mi NEM eredményezi az adatok végleges törlését?
    a) az adatok átmozgatása a Lomtárba
    b) a háttértároló elektromágneses törlése

c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

118. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

119. Mi a célja a a szoftverfrissítések telepítésének?
a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

120. Mi az oka a személyes adatok védelmének?
a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

121. Mi igaz a karanténban lévő fájlokra?
a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni