بنك أسئلة

(76 سؤالاً وجوابًا)

الدرس الثاني – الوحدة الأولى

الأمن السيبراني

لمادة المهارات الرقمية

الصف التاسع – الفصل الثاني

إعداد: الأستاذ الفاضل نزار الأخرس

منقول من قبل: منتديات صقر الجنوب التعليمية

اسئلة الدرس الثاني من الفصل الثاني لمادة المهارات الرقمية المنهاج الجديد للصف التاسع 76 سؤال

الوحدة الاولى الأمن السيبراني.

الأمن السيبراني. (76)132-57

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
57	من الأحداث الأمنية الخطيرة التى أدت الى ظهور وأهمية الأمن السيبراني هي :	تعرض شركة فيس بوك وهي شركة خدمات أمريكية لاثنين من أكبر إختراقات البيانات في التاريخ، حيث إخترقت بيانات 3مليارات حساب في 2013و 500مليون حساب في .2014	تعرض شركة ياهو وهي شركة خدمات أمريكية لاثنين من أكبر إختراقات البيانات في التاريخ، حيث إخترقت بيانات 3 مليارات حساب في 2013و 500مليون حساب في .2014	تعرض شركة امازون وهي شركة خدمات أمريكية لاثنين من أكبر إختراقات البيانات في التاريخ، حيث إخترقت بيانات 3 مليارات حساب في 2013و 500مليون حساب في .2014	تعرض شركة ياهو وهي شركة خدمات أمريكية لاثنين من أكبر السرقات في أمريكا، حيث تم سرقة كل سيرفرات الشركة وأجهزة حاسوب الموظفين المخزن عليها بيانات العاملين والمراجعين في عامي 2013و .2014	تعرض شركة ياهو وهي شركة خدمات أمريكية لاثنين من أكبر إختراقات البيانات في التاريخ، حيث إخترقت بيانات 3مليارات حساب في 2013و 500مليون حساب في .2014
58	تضمنت البيانات المسروقة عند اختراق أجهزة شركة ياهو عامي 2013و 2014 :	أسماء المستخدمين وكلمات المرور غير المشفرة.	أسماء المستخدمين وكلمات المرور المشفرة.	كلمات المرور فقط غير المشفرة.	أسماء المستخدمين فقط	أسماء المستخدمين وكلمات المرور غير المشفرة.
59	يتكون الأمن السيبراني من طبقات متعددة من الحماية، تأتى على شكل: المحتوى من اعداد الأستاذ الفاضل نزار الاخرس تم تجميع اللغة من قبل منتديات صقر الجنوب التعليمية	مجموعة من البرمجيات التى تعمل على فصل الشبكة في الأوقات الخارجة عن الدوام الرسمي.	مجموعة من موظفى الحماية المسؤولين عن حماية وتأمين أمن أجهزة السيرفر الخاصة بالشركة من أي هجوم الكترونى أو واقعي.	مجموعة من الممارسات والتقنيات والإجراءات التى تهدف إلى حماية الأنظمة والشبكات والبيانات والبنية التحتية الرقمية من الهجمات والإعتداءات الإلكترونية.	جميع ما ذُكر	مجموعة من الممارسات والتقنيات والإجراءات التى تهدف إلى حماية الأنظمة والشبكات والبيانات والبنية التحتية الرقمية من الهجمات والإعتداءات الإلكترونية.
60	حماية البيانات، سلامة النظام، توافر الخدمة والخصوصية ..هى من :	أوليات أي مبرمج خبير.	مهمات الطاقم الإداري في المؤسسات الحكومية.	أهداف الأمن السيبراني.	أهداف أمن المعلومات.	أهداف الأمن السيبراني.
61	من أهداف الأمن السيبراني :	حماية البيانات -توافر الخدمة -سلامة النظام -الخصوصية - اكتشاف الهجمات والإستجابة لها.	حماية الموظفين - تأمين بيئة عمل للخريجين -بناء الشركات والإستثمارات -الثقة.	القدرة والمهارة في الإختراق -تدريب الكادر على آليات الدخول الى أجهزة الشركات الأخرى -بناء مهارات عالية في	المهارة في إدارة موارد الشركات -زيادة حجم الإستثمارات وهامش الأرباح الذي ينشأ من زيادة وعي وقدرة الموظفين على	حماية البيانات - توافر الخدمة - سلامة النظام - الخصوصية - اكتشاف الهجمات والإستجابة لها.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
				الشبكات لدى الموظفين.	التعامل مع مواقع التواصل الإجتماعي.	
62	تأمين البيانات الحساسة والشخصية من الوصول غير المصرح به أو السرقة ..هي واحدة من أهداف :	الأمن السيبراني في حماية البيانات.	الأمن السيبراني في سلامة النظام.	الأمن السيبراني في توافر الخدمة	الأمن السيبراني في الخصوصية.	الأمن السيبراني في حماية البيانات.
63	ضمان أن الأنظمة والبرامج تعمل بشكل صحيح دون تعرضها للتلاعب أو الإختراق ..هي واحدة من أهداف :	الأمن السيبراني في حماية البيانات.	الأمن السيبراني في سلامة النظام.	الأمن السيبراني في توافر الخدمة	الأمن السيبراني في الخصوصية.	الأمن السيبراني في سلامة النظام.
64	الحفاظ على إستمرارية الخدمات والتطبيقات من الإنقطاع أو التعطل الناتج عن الهجمات ..هي واحدة من أهداف :	الأمن السيبراني في حماية البيانات.	الأمن السيبراني في سلامة النظام. المحتوى من اعداد الأستاذ الفاضل نزار الوغرس تم تجميع الملف من قبل منتديات صقر الجنوب التعاونية	الأمن السيبراني في توافر الخدمة	الأمن السيبراني في الخصوصية.	الأمن السيبراني في توافر الخدمة
65	حماية المعلومات الشخصية من الكشف أو الإستخدام غير المصرح به ..هي واحدة من أهداف :	الأمن السيبراني في حماية البيانات.	الأمن السيبراني في سلامة النظام.	الأمن السيبراني في توافر الخدمة	الأمن السيبراني في الخصوصية.	الأمن السيبراني في الخصوصية.
66	في سياق حماية المملكة من تهديدات الأمن السيبراني، ومواجهتها في بكفاءة وفعالية لضمان استدامة العمل، والحفاظ على الأمن الوطني، وسلامة الأشخاص والممتلكات والمعلومات، قامت الحكومة ب :	وضع خطة بديلة لعمل شبكة محلية وطنية مستقلة عن شبكة الإنترنت مما يضمن وقف عمليات الإختراق والتطفل.	الإستغناء عن العمل ضمن شبكة الويب العالمية.	فصل الأجهزة الرئيسية والخوادم بعد إنتهاء وقت الدوام.	انشاء المركز الوطني للأمن السيبراني وتدريب موظفي القطاع العام والخاص وفئات المجتمع الأخرى وتأهيلهم وتوعيتهم وإكسابهم المعرفة والمهارات للحد من المخاطر والتهديدات.	انشاء المركز الوطني للأمن السيبراني وتدريب موظفي القطاع العام والخاص وفئات المجتمع الأخرى وتأهيلهم وتوعيتهم وإكسابهم المعرفة والمهارات للحد من المخاطر والتهديدات.
67	هي محاولات أو إجراءات خبيثة تهدف الى إلحاق الضرر بأنظمة المعلومات، أو الشبكات، أو البيانات الخاصة	Cyber Security Courses.	Cyber Security Threats.	Cyber Security Technician.	Cyber Security Tutorial.	Cyber Security Threats.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
	بالمؤسسات، أو الأفراد.					
68	تهدف تهديدات الأمن السيبراني الى :	التلاعب بالمعلومات.	سرقة المعلومات.	إتلاف المعلومات.	جميع ما ذُكر	جميع ما ذُكر
69	يمكن أن تكون تهديدات الأمن السيبراني من:	مصادر داخلية أو خارجية أو منظمات أو أفراد.	مصادر داخلية، أو أفراد فقط.	مصادر خارجية، أو منظمات فقط.	مصادر داخلية، أو منظمات فقط.	مصادر داخلية أو خارجية أو منظمات أو أفراد.
70	وهي برامج ضارة تصيب الأنظمة بهدف التدمير أو التجسس أو سرقة البيانات، ويمكن أن تؤدي الى فقدان البيانات، وتعطيل الأنظمة، وسرقة المعلومات الحساسة.	Malware.	Phishing. المحتوى من اعداد الأستاذ الفاضل نزار الدغرس تم تجميع اللغة من قبل منتديات صقر الجنوب التعليمية	Security Vulnerabilities.	Distributed Denial of Service.	Malware.
71	Viruses, Worms, Ransomware and Spyware ... are Examples for:	Security Vulnerabilities.	Phishing.	Malware.	Distributed Denial of Service.	Malware.
72	Examples for Milware:	Viruses, Worms, Bacteria and Fungi.	Viruses, Worms, Ransomware and Spyware.	Viruses, Worms, Bacteria and Germs.	Viruses, Worms, Bacteria,Protozoa.	Viruses, Worms, Ransomware and Spyware.
73	تصيب الملفات والبرامج، وتتاكاثر عند تشغيل الملف المصاب.	Viruses.	Worms.	Ransomware.	Spyware.	Viruses.
74	تنتشر عبر الشبكات وتستغل الثغرات الأمنية دون الحاجة الى تفاعل المستخدم.	Viruses.	Worms.	Ransomware.	Spyware.	Worms.
75	تُقفل الأنظمة أو تُشفر البيانات، وتُطلب فدية لإعادتها.	Viruses.	Worms.	Ransomware.	Spyware.	Ransomware.
76	تراقب نشاط المستخدم وتسرق المعلومات الحساسة دون علمه.	Viruses.	Worms.	Ransomware.	Spyware.	Spyware.
77	Trojan Horse is:	Virus.	Worm.	Ransomware.	Malware.	Malware.
78	هى محاولات احتيالية للحصول	Malware.	Phishing.	Security Vulnerabilities.	Distributed Denial of Service.	Phishing.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
	على معلومات حساسة عن طريق تقمص هوية جهات موثوقة عبر البريد الإلكتروني، أو الرسائل النصية أو المواقع المزيفة.					
79	يمكن أن يؤدي التصيد الإحتيالي الى :	فقدان المعلومات المالية.	سرقة الهوية.	الإختراقات الأمنية.	جميع ما ذُكر	جميع ما ذُكر
80	في الصورة المرفقة مع السؤال فان آلية العمل الموضحة توضح واحدة من أنواع تهديدات الأمن السيبراني من النوع :	Malware.	Phishing.	Security Vulnerabilities.	Distributed Denial of Service.	Phishing.
81	هي نقاط ضعف أو عيوب في الأنظمة أو البرامج أو الشبكات، يمكن أن تُستغل من قبل المهاجمين لإختراق النظام والوصول الى بيانات حساسة، أو القيام بتصرفات ضارة.	Malware.	Phishing. المحتوى من اعداد الأستاذ الفاضل نزار الاخرس تم تجميع الملف من قبل منتديات صقر الجزيرة التعليمية	Security Vulnerabilities.	Distributed Denial of Service.	Security Vulnerabilities.
82	هي نوع من أنواع الثغرات الأمنية وتحدث نتيجة وجود أخطاء في كتابة الكود البرمجي، أو ثغرات في التعامل مع المدخلات غير الموثوقة.	Software Vulnerabilities.	Network Vulnerabilities.	Procedural Vulnerabilities.	Hardware Vulnerabilities.	Software Vulnerabilities.
83	هي نوع من أنواع الثغرات الأمنية، تشمل نقاط ضعف في تكوينات الشبكة أو البروتوكولات، مثل ضعف بروتوكلات التشفير (SSL / TLS) أو الشبكات اللاسلكية غير المؤمنة.	Software Vulnerabilities.	Network Vulnerabilities.	Procedural Vulnerabilities.	Hardware Vulnerabilities.	Network Vulnerabilities.
84	هي نوع من أنواع الثغرات الأمنية، تتعلق بكيفية تنفيذ العمليات، ويمكن أن	Software Vulnerabilities.	Network Vulnerabilities.	Procedural Vulnerabilities.	Hardware Vulnerabilities.	Procedural Vulnerabilities.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
	تؤدي الى مخاطر أمان، أو فقدان البيانات، أو إنتهاك خصوصية، مثل ضعف إجراءات التحقق من الهوية، وعدم وجود خطوات كافية لتأكيد هوية المستخدمين قبل منحهم الوصول الى الأنظمة.			المحتوى من اعداد الأستاذ الفاضل نزار الادغرس تم تجميع الملف من قبل منتديات صقر الجنوب التعاونية		
85	هي نوع من أنواع الثغرات الأمنية، تشمل نقاط ضعف في المعدات، مثل معالجات الحواسيب، وأحد أشهر الأمثلة هى ثغرات (Meltdown Spectre)التى أثرت في معالجات شركات عدة.	Software Vulnerabilities.	Network Vulnerabilities.	Procedural Vulnerabilities.	Hardware Vulnerabilities.	Hardware Vulnerabilities.
86	SSL / TLS...	هي من بروتوكولات التراسل على الشبكة.	هو بروتوكول نقل النص التشعبي.	هو بروتوكول الإنترنت.	هي بروتوكولات التشفير.	هي بروتوكولات التشفير.
87	المكان التى تستهدفه Meltdown Spectreهو :	التطبيقات.	الهارد ديسك.	المعالجات.	ذاكرة الوصول العشوائي.	المعالجات.
88	هي مجموعة من الأدوات والبرمجيات مفتوحة المصدر، تُستخدم لتوفير الأمان والتشفير في الإتصالات عبر الإنترنت.	Heartbleed.	OpenSSL.	TLS.	HTTP.	OpenSSL.
89	هي من إحدى أشهر الثغرات الأمنية التي أثرت في مكتبة OpenSSLالمكتشفة في 2014والتى سمحت للمهاجمين سرقة معلومات حساسة من الذاكرة.	Worm.	Heartbleed.	Meltdown Spectre.	Malware.	Heartbleed.
90	تستهدف هذه الثغرة البرمجيات مفتوحة المصدر.	Meltdown Spectre.	OpenSSL.	Worms.	Heartbleed.	Heartbleed.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
91	DDoS.. Stands for :	Distributed Denial of Service.	Distributed Database System.	Distributed Database Open Source.	Docmented Database Open Source.	Distributed Denial of Service.
92	هو الهجوم الذي يتم فيه إغراق نظام أو خادم معين بعدد هائل من الطلبات بشكل متزامن من مصادر موزعة عدة، بهدف إيقاف النظام أو جعله غير قادر على الإستجابة للمسخدمين الشرعيين.	Heartbleed.	DOS (Disk Operation System).	Meltdown Spectre.	Distributed Denial of Service.	Distributed Denial of Service.
93	هو نوع من هجمات Dos :	Heartbleed.	Meltdown Spectre.	DDoS.	OpenSSL.	DDoS.
94	Botnet is:	شبكة من الأجهزة المخترقة التى يتم تنفيذ هجمات DDos عليها.	شبكة المساحة المحلية الخاصة بالشركات.	الشبكة العنكبوتية العالمية.	شبكة من أجهزة الشركة التى تحتوي على خلل تقنى وفنى ويكون فيها قطع، مما يمنع وصول البيانات بين الأجهزة.	شبكة من الأجهزة المخترقة التى يتم تنفيذ هجمات DDosعليها.
95	تُنفذ هذه الهجمات باستخدام شبكة من الأجهزة المخترقة، ويُتحكم بها عن بعد من قبل المهاجمين، وقد تكون هذه الهجمات على مستوى الشبكة أو على مستوى التطبيق أو على مستوى البيانات.	DDoS.	OpenSSL.	Meltdown Spectre.	Distributed Database Open Source.	DDoS.
96	في الصورة المرفقة مع السؤال فان الآلية الموضحة توضح مبدأ عمل :	Heartbleed.	Identity Theft.	DDoS.	Meltdown Spectre.	DDoS.
97	في الصورة المرافقة مع السؤال، فان الآلية الموضحة توضح مبدأ عمل :	Heartbleed.	Identity Theft.	DDoS.	Meltdown Spectre.	Identity Theft.
98	وتعنى استخدام معلومات شخصية مسروقة، مثل الإسم، وتاريخ الميلاد، ورقم الهوية أو الضمان	Identity Theft.	DDoS.	OpenSSL.	Meltdown Spectre.	Identity Theft.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
	الإجتماعي، أو معلومات مالية، مثل أرقام الحسابات المصرفية، وبطاقات الإئتمان لتمثيل شخص آخر دون إذنه.					
99	يؤدي التهديد السيبراني من نوع سرقة الهوية الى:	تعطيل خدمات الموقع الإلكتروني المستهدف عن طريق إغراق النظام بطلبات أكثر من التى يمكنه التعامل معها.	خسائر مالية، وأضرار بالسمعة، وتعقيدات قانونية للضحية.	سرقة الوثائق الشخصية الرسمية الورقية.	تعطيل مزود خدمة الإنترنت للضحية، مما يؤدي الى فصله عن شبكة الإنترنت.	خسائر مالية، وأضرار بالسمعة، وتعقيدات قانونية للضحية.
100	تكون هجمات حجب الخدمة الموزعة على مستوى :	الشبكة -التطبيق - البيانات.	الشبكة -المعالجات -ذاكرة الوصول العشوائي.	أسلاك الشبكة - البيانات -التطبيقات.	الشبكة المحلية - التطبيقات - البرمجيات.	الشبكة -التطبيق - البيانات.
101	هى تقنية احتيالية تعتمد على التلاعب النفسى بالأفراد لاستدراجهم للكشف عن معلومات حساسة، أو القيام بأفعال معينة تساعد المهاجمين على اختراق الأنظمة أو سرقة البيانات .	Identity Theft.	Social Engineering.	DDoS.	Meltdown Spectre.	Social Engineering.
102	يعتمد المهاجمون في هذه الطريقة على استغلال الثقة والخداع والتلاعب في العواطف والسلوكات البشرية.	Social Engineering.	Identity Theft.	DDoS.	Meltdown Spectre.	Social Engineering.
103	في الصورة المرافقة مع السؤال، ما هو الترتيب الصحيح لخطوات التهديد الخاصة بالهندسة الإجتماعية؟	1	2	3	4	3
104	يكون هذا النوع من التهديد أكثر تركيزاً على التسبب في ضرر مباشر وفوري للضحية بنية خبيثة واضحة.	الهجوم الإلكتروني.	الإعتداء الإلكتروني.	حجب الخدمة الموزعة.	التسوق الإلكتروني.	الإعتداء الإلكتروني.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
105	الفرق بين الهجوم الإلكتروني والإعتداء الإلكتروني هو:	أن الإعتداء الإلكتروني يشمل أي محاولة غير مشروعة للوصول إلى الأنظمة الرقمية أو تعطيلها، بينما الهجوم الإلكتروني يكون أكثر تركيزاً على التسبب في ضرر مباشر وفوري للضحية بنية خبيثة واضحة.	أن الهجوم الإلكتروني يشمل أي محاولة غير مشروعة للوصول إلى الأنظمة الرقمية أو تعطيلها، بينما الإعتداء الإلكتروني يكون أكثر تركيزاً على التسبب في ضرر مباشر وفوري للضحية بنية خبيثة واضحة.	ليس هناك أي فرق بين النوعين، حيث يحاول المعتدي الإلكتروني عند إختراق أنظمة الضحية الإطلاع على البيانات الشخصية كنوع من أنواع التطفل لا أكثر.	جميع ما ذُكر.	أن الهجوم الإلكتروني يشمل أي محاولة غير مشروعة للوصول إلى الأنظمة الرقمية أو تعطيلها، بينما الإعتداء الإلكتروني يكون أكثر تركيزاً على التسبب في ضرر مباشر وفوري للضحية بنية خبيثة واضحة.
106	يُمكن أن تكون الإعتداءات الإلكترونية جزءاً من الهجمات الإلكترونية، لكنها تتميز بتركيزها على الأضرار الشخصية والمباشرة.	جملة صحيحة.	جملة خاطئة.	0 المحتوى من اعداد الأستاذ الفاضل نزار الادهمي تم تجميع الملف من قبل منتديات صقر الجنوب التعليمية	0	جملة صحيحة.
107	تشمل وسائل الحماية من تهديدات الأمن السيبراني:	الحماية المادية والمالية.	الحماية المادية والرقمية.	الحماية الشخصية والعائلية.	الحماية الأمنية والإجتماعية.	الحماية المادية والرقمية.
108	يهدف هذا النوع من الحماية إلى تأمين الأجهزة المادية والمعدات التي تُستخدم في تخزين البيانات ومعالجتها، وتضمن حماية البنية التحتية المادية للأنظمة.	Physical Security.	Digital Security.	Operational Security.	Management Security	Physical Security.
109	وهي الوسائل المستخدمة لحماية البيانات والأنظمة الإلكترونية من الهجمات الإلكترونية، وهي تتعلق بالحماية التقنية التي تشمل الدفاع ضد الإختراقات، والبرامج الضارة، وسرقة البيانات، وغيرها من التهديدات التي تستهدف الأنظمة الرقمية.	Physical Security.	Digital Security.	Operational Security.	Management Security	Digital Security.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
110	وتشمل هذه الوسائل الإجراءات التى تمنع الوصول غير المصرح به الى الأماكن التى تحتوي على المعدات الإلكترونية والبيانات الحساسة.	Digital Security.	Identity Theft.	Social Engineering.	Physical Security.	Physical Security.
111	إستخدام الأقفال والمفاتيح والأجهزة البيومترية لتقييد الوصول الى المرافق والمعدات الحساسة .هي وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل المالية.	الوسائل الإجتماعية.	الوسائل المادية.
112	استخدام الكاميرات الأمنية لمراقبة المداخل والمناطق الحساسة .هي وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل التقليدية.	الوسائل التقليدية.	الوسائل المادية.
113	توظيف حراس أمن لتأمين المرافق والتحقق من هويات الزوار .هى وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل التقنية.	الوسائل المالية.	الوسائل المادية.
114	تدابير حماية المعدات والبنية التحتية من الكوارث، مثل الحرائق والزلازل والفيضانات .هى وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل غير المفيدة.	الوسائل غير المفيدة.	الوسائل المادية.
115	التشفير .هي وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل التعليمية	الوسائل الإجتماعية.	الوسائل الرقمية.
116	المصادقة متعددة العوامل .هى وسيلة من وسائل الحماية	الوسائل الرقمية.	الوسائل المادية.	الوسائل التعليمية	الوسائل المالية.	الوسائل الرقمية.

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
	من تهديدات الأمن السيبراني من نوع :					
117	جدران الحماية .هي وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل غير المفيدة.	الوسائل التعليمية	الوسائل الرقمية.
118	البرامج المضادة للفيروسات .هى وسيلة من وسائل الحماية من تهديدات الأمن السيبراني من نوع :	الوسائل الرقمية.	الوسائل المادية.	الوسائل الإجتماعية.	الوسائل التعليمية	الوسائل الرقمية.
119	واحدة من الآتية جملة صحيحة فيما يتعلق بالوسائل المادية للحماية من تهديدات الأمن السيبراني.	التشفير.	المصادقة متعددة العوامل.	الحراس الأمنيون.	جدران الحماية.	الحراس الأمنيون.
120	واحدة من الآتية جملة صحيحة فيما يتعلق بالوسائل الرقمية للحماية من تهديدات الأمن السيبراني.	ضوابط الوصول الفيزيائي.	المراقبة بالفيديو.	الحراس الأمنيون. المحتوى من اعداد الأستاذ الفاضل نزار ادهرس تم تجميع الملف من قبل منتديات صقر الجنوب التعاونية	المصادقة متعددة العوامل.	المصادقة متعددة العوامل.
121	MFA.. Stands for :	Multi-Factor Authentication.	Multimedia Filter Air.	Multifunctional Fitness Aerobic step platform.	Multi Flight Airlines.	Multi-Factor Authentication.
122	معنى الأجهزة البيومترية المستخدمة في الوسائل المادية من وسائل الحماية في الحماية من تهديدات الأمن السيبراني هو :	بصمات الأصابع أو ماسحات الوجه.	كلمات السر والتوقيع الإلكتروني.	أجهزة قياس الضغط الجوي وضغط الدم الخاص بالموظفين.	اخذ عينات دم من الموظفين للتأكد من عدم وجود فيروسات تؤدي الى العدوى.	بصمات الأصابع أو ماسحات الوجه.
123	Phyisical Access Control is:	استخدام الأقفال والمفاتيح والأجهزة البيومترية لتفييد الوصول الى المرافق والمعدات الحساسة.	استخدام الكاميرات الأمنية لمراقبة المداخل والمناطق الحساسة.	توظيف حراس أمن لتأمين المرافق والتحقق من هويات الزوار -تدابير لحماية المغدات والبنية التحتية من الكوارث مثل الحرائق والزلازل والفيضانات.	جميع ما ذُكر.	استخدام الأقفال والمفاتيح والأجهزة البيومترية لتفييد الوصول الى المرافق والمعدات الحساسة.
124	Video Surveillance is:	استخدام الأقفال والمفاتيح والأجهزة	استخدام الكاميرات الأمنية لمراقبة	توظيف حراس أمن لتأمين المرافق	تدابير لحماية المعدات والبنية	استخدام الكاميرات الأمنية لمراقبة

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
		البيومترية لتفييد الوصول الى المرافق والمعدات الحساسة.	المداخل والمناطق الحساسة.	والتحقق من هويات الزوار.	التحتية من الكوارث مثل الحرائق والزلازل والفيضانات.	المداخل والمناطق الحساسة.
125	Security Guards is:	استخدام الأقفال والمفاتيح والأجهزة البيومترية لتفييد الوصول الى المرافق والمعدات الحساسة.	استخدام الكاميرات الأمنية لمراقبة المداخل والمناطق الحساسة.	توظيف حراس أمن لتأمين المرافق والتحقق من هويات الزوار.	تدابير لحماية المغدات والبنية التحتية من الكوارث مثل الحرائق والزلازل والفيضانات.	توظيف حراس أمن لتأمين المرافق والتحقق من هويات الزوار.
126	Disaster Protection is:	استخدام الأقفال والمفاتيح والأجهزة البيومترية لتفييد الوصول الى المرافق والمعدات الحساسة.	استخدام الكاميرات الأمنية لمراقبة المداخل والمناطق الحساسة.	توظيف حراس أمن لتأمين المرافق والتحقق من هويات الزوار.	تدابير لحماية المغدات والبنية التحتية من الكوارث مثل الحرائق والزلازل والفيضانات.	تدابير لحماية المغدات والبنية التحتية من الكوارث مثل الحرائق والزلازل والفيضانات.
127	التكامل الوظيفي بين الوسائل المادية والرقمية لحماية البيانات أدى الى :	وجود ثغرات في الأنظمة .	زيادة نقاط الضعف.	زيادة الإختراقات الأمنية بسبب زيادة الثغرات الناتجة عن هذا التكامل.	تقليل من نقاط الضعف، وضمان أماناً متكاملاً للبيانات المتبادلة.	تقليل من نقاط الضعف، وضمان أماناً متكاملاً للبيانات المتبادلة.
128	التشفير واستخدام برامج الحماية من الفيروسات وبرامج مكافحة الإختراق وتفعيل جدران الحماية والتحديثات الأمنية ..هي من إجراءات :	الأمان الرقمي.	الأمان المادي.	الأمان الشخصي والمالي.	الأمان الوظيفي.	الأمان الرقمي.
129	الحماية المادية للأجهزة والتخلص الآمن من البيانات .. هى من إجراءات :	الأمان الرقمي.	الأمان المادي.	الأمان الشخصى والمالي.	الأمان الوظيفي.	الأمان المادي.
130	التخلص من البيانات الحساسة بشكل آمن من الأجهزة لمنع إستردادها ..هو :	من مساوئ الأمان المادي.	من مساوئ الأمان الرقمي.	من إجراءات الأمان المادي.	من مظاهر التهديدات والإختراقات الأمنية.	من إجراءات الأمان المادي.
131	من الممارسات الجيدة للأمان :	كلمات مرور قوية - التوعية الأمنية - النسخ الإحتياطي للبيانات -خطط الإستجابة للحوادث .	عدم إستخدام كلمات المرور -التدرب على مهارات الإختراق - تخزين نسخة من كلمات السر في أكثر من مكان.	استخدام بديل عن كلمات المرور التقليدية -التواصل مع المخترقين والتعرف على آليات العمل لحماية الأجهزة الشخصية وأجهزة الشركة -تخزين نسخ احتياطية على سطح المكتب.	عدم كتابة كلمة المرور في أي مكان -عدم القيام بعمل أي نسخة احتياطية للبيانات الحساسة للحرص على عدم وصول المخترقين لها - التدرب على مهارات الإختراق.	كلمات مرور قوية - التوعية الأمنية - النسخ الإحتياطي للبيانات -خطط الإستجابة للحوادث .

Num	السؤال	الخيار الأول	الخيار الثاني	الخيار الثالث	الخيار الرابع	الحل
132	يمكن الإستفادة من أدوات الأمن السيبراني والذكاء الإصطناعي والتعلم الآلي في :	اكتشاف التهديدات والإستجابة لها بشكل أسرع من البشر .	تحليل الأنماط والتنبؤ بالهجمات المحتملة.	حماية البيانات الحساسة.	جميع ما ذُكر.	جميع ما ذُكر.


منتديات صقر الجنوب
المملكة الأردنية الهاشمية
www.jnob-jo.com