المملكة العربية السعودية

العطاء الرقمي
Attaa Digital

مسابقة ليالي العطاء الرمضانية

الحقيبة التدريبية لبرنامج

حماية الهوية الالكترونية

بقيادة المدرب:.....

١٤٤١هـ

المملكة العربية السعودية

العطاء الرقمي
Attaa Digital

مسابقة
ليالي
العطاء الرمضانية

دليل المدرب لبرنامج

حماية الهوية الالكترونية

بقيادة المدرب:.....

١٤٤١هـ


بسم الله الرحمن الرحيم

الفهرس

المقدمة

عزيزي المدرب ...

الأطفال هم أمانه ولابد أن نحميهم من خطر العالم الالكتروني و نضيف مفهوم الأمن السيبراني الى ثقافتهم الرقمية بطريقه محبب و متدرجة .

لذلك نأمل منك عزيزي المدرب تعريف الأطفال المتدربين بماهية الهوية الالكترونية وأهميتها بالإضافة تعريفهم بالأساليب التي يتبعها المنتحلون و تأهيلهم للقيام بدورهم في تطبيق طرق الوقاية و الأمان و الحفاظ على معلوماتهم الشخصية.

دمت موفقاً

إرشادات للمدرب

- التحضير الجيد و التمكن من المادة العلمية المعدة في هذه الحقيبة.
- التأكد من توفر جميع الأدوات قبل بدء الدورة .
- توزيع الأقلام و الأوراق و اللافتات على الطاولات قبل بدء الدورة.
- توزيع الأطفال المتدربين الى مجموعات مناسبة لا تقل عن خمسة أطفال.
- التعرف على الأطفال المتدربين .
- اختيار عشوائي للمتدربين اثناء طرح الأسئلة و النقاش.
- ركز على احتياجات الأطفال.
- في النقاش شجع المتدربين على الأسئلة و تبادل الخبرات.
- لا تقرأ مباشرة من العرض.
- اختار عبارات بسيطة تتناسب مع المرحلة العمرية للأطفال.

دليل
البرنامج التدريبي
الزمن الكلي : ١٨٠ دقيقة

م	الجلسة الاولى	الراحة	الجلسة الثانية
المواضيع	• معنى الهوية الالكترونية . • كيف نحمي بياناتنا على مواقع التواصل الاجتماعي. • التعرف على طرق سرقة الهوية الالكترونية.	٣٠ دقيقة	• كيف نحمي بياناتنا في : ١. شبكات الواي فاي العامة. ٢. من خطر برمجيات الدعاية و الإعلانات. ٣. تقنية البلوتوث. • نظام مكافحة الجرائم المعلوماتية.
الزمن	٧٥ دقيقة		٧٥ دقيقة

دليل الجلسات

الجلسة الأولى

الزمن :٧٥ دقيقة

أولاً: محاور الجلسة الأولى:

- كيف نحمي بياناتنا في:
  ١. شبكات الواي فاي العامة.
  ٢. من خطر برمجيات الدعاية و الإعلانات.
  ٣. تقنية البلوتوث.
- نظام مكافحة الجرائم المعلوماتية.

ثانياً: أهداف الجلسة:

يتوقع في نهاية الجلسة أن يكون الطفل قادراً على:

١. ان يعرف معنى الهوية الالكترونية و الهوية الحقيقية و يفرق بينهما.
٢. ان يحدد ماهي المعلومات الشخصية التي يشاركها على مواقع التواصل الاجتماعي.
٣. ان يتعرف على طرق و أساليب سرقة الهوية الالكترونية.

ثالثاً: الأساليب و الأنشطة و الوسائل التدريبية:

مناقشات فردية – مناقشات جماعية و ورش عمل – شرح

الجلسة الأولى

الزمن :٧٥ دقيقة

رابعاً: دليل الجلسة الأولى:

الجلسة	العنصر		الزمن مفصلاً للعنصر	الزمن الكلي
الأولى	الترحيب و التعارف		١٠ دقيقة	
	معنى الهوية الالكترونية .		١٠دقائق	
	كيف نحمي بياناتنا على مواقع التواصل الاجتماعي.	نقاش١	٥ دقائق	١٥ دقيقة
			٥دقائق	
		نشاط١	٥دقائق	
	التعرف على طرق سرقة الهوية الالكترونية.	نقاش٢	٥ دقائق	٤٥ دقيقة
		الطرق	٢٥ دقيقه	
		نشاط ٢	١٠ دقيقة	

الجلسة الثانية

الزمن :٧٥ دقيقة

أولاً: محاور الجلسة الأولى:

١. معنى الهوية الالكترونية .
٢. كيف نحمي بياناتنا على مواقع التواصل الاجتماعي.
٣. التعرف على طرق سرقة الهوية الالكترونية.

ثانياً: أهداف الجلسة:

يتوقع في نهاية الجلسة أن يكون الطفل قادراً على:

١. أن يحمي نفسة في الشبكات اللاسلكية العامة.
٢. ان يتعرف على برمجيات الدعاية و الإعلانات وكيفية الوقاية منها.
٣. أن يحمي نفسة في تقنيات البلوتوث.
٤. ان يعرف أن هناك قانون يحميه في حال تعرض للانتحال وهو قانون الجرائم الالكترونية.

ثالثاً: الأساليب و الأنشطة و الوسائل التدريبية:

مناقشات فردية – مناقشات جماعية و ورش عمل – شرح.

الجلسة الثانية

الزمن :٧٥ دقيقة

رابعاً: دليل الجلسة الثانية:

الجلسة	العنصر		الزمن مفصلاً للعنصر	الزمن الكلي
الثانية	مراجعة سريعة لما سبق			١٠دقائق
	كيف نحمي بياناتنا في الشبكات اللاسلكية العامة		٨ دقائق	١٠دقائق
		نقاش٣	دقيقتين	
	كيف نحمي بياناتنا من خطر برمجيات الدعاية و الإعلانات.			١٠دقائق
	كيف نحمي بياناتنا في تقنية البلوتوث.			١٠دقائق
	نظام مكافحة الجرائم المعلوماتية.			١٥دقيقة
	مراجعة لما تم دراسته في الدورة	نشاط٣		١٠ دقيقة
	الأسئلة و الختام			١٠دقيقة

انتهى دليل المدرب

المملكة العربية السعودية

العطاء الرقمي
Attaa Digital

مسابقة ليالي العطاء الرمضانية

الحقيبة التدريبية لبرنامج

حماية الهوية الالكترونية

بقيادة المدرب:.....

١٤٤١هـ

المملكة العربية السعودية

العطاء الرقمي
Attaa Digital

مسابقة ليالي العطاء الرمضانية

دليل المتدرب لبرنامج

حماية الهوية الالكترونية

بقيادة المدرب:.....

١٤٤١هـ


بسم الله الرحمن الرحيم

الفهرس

المقدمة

يسرنا أن نرحب بكم في هذا البرنامج التدريبي
"حماية الهوية الالكتروني"

حيث نأخذكم في رحلة مثيرة و ممتعه يجتمع فيها العلم و المتعة.
سائلين المولى عز وجل أن يوفقنا في تقديم المادة لزيادة وعيكم بما يتماشى مع متطلبات العصر.

بطاقة التعارف

الاسم:.....

العمر:.....

المرحلة الدراسية:.....

الهوايات:.....

تحدث عن نفسك:

.....

.....

.....

.....

التعريف بالبرنامج

الوقت: ٣ساعات مقسمة كالتالي:

- الجلسة التدريبية الأولى ٧٥ دقيقة.
- راحة ٣٠ دقيقة.
- الجلسة التدريبية الأولى ٧٥ دقيقة.

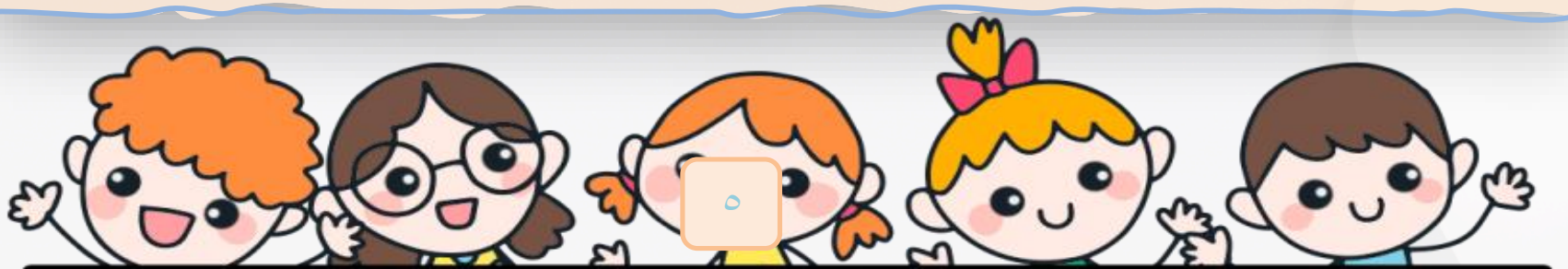
الأيام: يوم واحد فقط.

الفئة العمرية: البرنامج يستهدف الفئة العمرية من ٩سنوات الى ١٢سنة.

نظام البرنامج التدريبي: مناقشات فردية – مناقشات جماعية و ورش عمل – شرح.
و يقسم الأطفال الى مجموعات لا تقل عن ٥ أطفال متدربين.

إرشادات للمتدرب

- كن مشاركاً في جميع الأنشطة و النقاشات.
- احترم المدرب و الزملاء و أفكارهم.
- احترم الوقت.
- تعاون مع مجموعتك وتبادل معهم القرارات اثناء النقاش و الأنشطة الجماعية.
- احرص على تطبيق ما تعلمته في حياتك.
- الإغلاق التام للجوال داخل القاعة التدريبية.



الجلسات التدريبية

م	الجلسة الاولى	الجلسة الثانية
عناصر الجلسات	• معنى الهوية الالكترونية . • كيف نحمي بياناتنا على مواقع التواصل الاجتماعي. • التعرف على طرق سرقة الهوية الالكترونية.	• كيف نحمي بياناتنا في : ١. شبكات الواي فاي العامة. ٢. من خطر برمجيات الدعاية و الإعلانات. ٣. تقنية البلوتوث. • نظام مكافحة الجرائم المعلوماتية.

عناصر و أهداف
الجلسة التدريبية الاولى

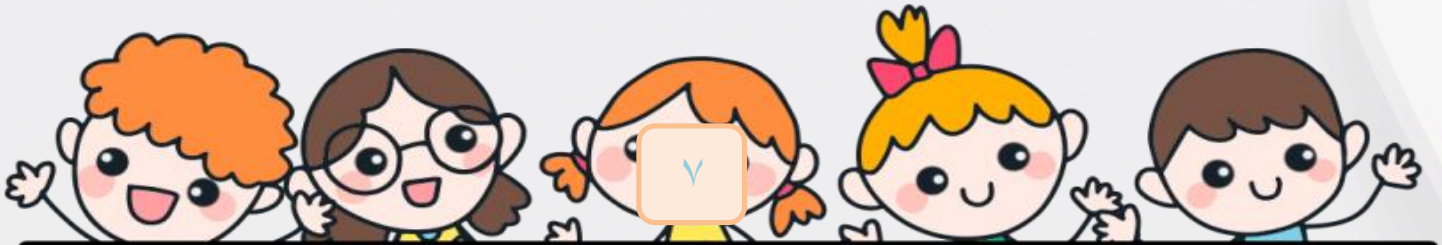
عناصر الجلسة:

- معنى الهوية الالكترونية .
- كيف نحمي بياناتنا على مواقع التواصل الاجتماعي.
- التعرف على طرق سرقة الهوية الالكترونية.
  ١. الهندسة الاجتماعية.
  ٢. التخمين.
  ٣. الثغرات.
  ٤. الخداع.

أهداف الجلسة:

يتوقع في نهاية الجلسة :

١. ان تعرف معنى الهوية الالكترونية و الهوية الحقيقية و تفرق بينهما.
٢. ان تحدد ماهي المعلومات الشخصية التي تشاركها على مواقع التواصل الاجتماعي.
٣. ان تتعرف على طرق و أساليب سرقة الهوية الالكترونية.



المادة العلمية للجلسة الاولى

الهوية الالكترونية

المعلومات الشخصية

- الهوية الحقيقية
- الهوية الإلكترونية

الهوية الحقيقية

هي التي يعرفك بها عائلتك و اصدقائك في المحيط الذي تعيش فيه مثل عمرك و عنوانك الحقيقي

الهوية الإلكترونية

هي التي تدخل بها الى العالم الرقمي و التي تظهر بها للآخرين على شبكة الانترنت و يفترض ان تكون قليلة للغاية .

نقاش ١

ما رأيك في مشاركة موقعك في برنامج السناب شات
أو الإنستغرام و لماذا ؟

.....

.....

.....

.....

.....

كيف نحمي بياناتنا و خصوصيتنا في مواقع التواصل الاجتماعي

SOCIAL MEDIA ICONS

في شبكات التواصل الاجتماعي

- لا تشارك إلا بالقليل من المعلومات .
- لا تكمل ملفك الشخصي على مواقع التواصل الاجتماعي و قم بإعطاء أقل معلومة ممكنة.
- تأكد أن من يطلع على انشطتك في شبكات التواصل هم فعلاً اصدقائك ومن تريد أن يتابعونك.

نشاط ١

بشكل فردي :خلال دقيقتين :

اذكري شبكات التواصل الاجتماعي التي تفضلينها ؟

.....

.....

.....

ماهي المعلومات الشخصية التي تشاركينها متابعيك ؟

.....

.....

.....

نقاش ٢

ماذا يريد المهاجمون منك ؟

.....

.....

.....

.....

.....

نقاش ٢

ماذا يريد المهاجمون منك ؟

- قد يستخدم احد حساباتك في إساءة الاستخدام و التخريب.
- التنمر الالكتروني سواء عليك او على زملائك.
- الاستفادة من الاشتراكات في البرامج المدفوعة.
- تتبع نشاطاتك و مواقعك وتهديدك بها.

.....الخ

طرق سرقة الهوية الالكترونية

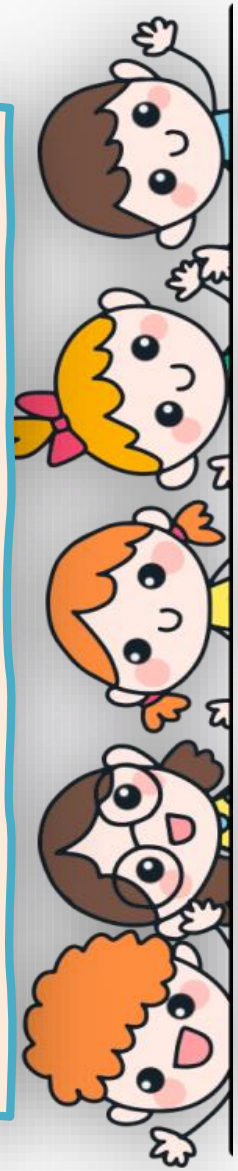
- الهندسة الاجتماعية
- استغلال الثغرات
- تخمين كلمات السر لشبكة الواي فاي
- الخداع

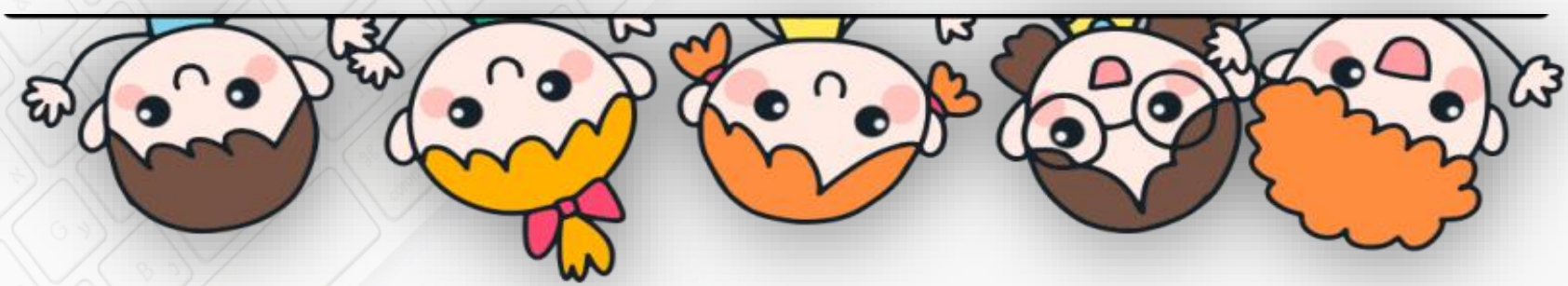
الهندسة الاجتماعية

هي الطرق الاجتماعية المختلفة للوصول الى الشخص و إقناعه في تنفيذ فعل ما أو الادلاء بمعلومات سرية

طرق الهندسة الاجتماعية

- الكذب و الخداع لسرقة كلمات سرية
- تتبع الاشخاص ومحاولة الدخول معهم في الانظمة
- شيء مقابل شيء





الخداع :

يرسل المهاجم رسالة على انها من مصدر موثوق و الرسالة تقنع المستخدم بمشاركة معلوماته المالية أو تثبيت برنامج خبيث

أحذر أن

- تفتح أي مرفق في البريد الالكتروني او رسالة سواء نصية أو واتس الا اذا كان المرسل معروف لديك
- تستجيب لأي رسالة طلب اذا لم تفهم معناها و أخبر أحد والديك
- ترسل بياناتك الشخصية و بيانات البطاقات البنكية .

تخمين كلمات السر لشبكات الواي فاي

يجب أن تحتوي جميع أجهزتنا على كلمات سر قوية حتى لا يستطيع المتطفل تخمين كلمات السر ثم الوصول على بياناتنا الشخصية

تخمين كلمات السر لشبكة الواي فاي

نشاط ٢

خلال دقيقة كل مجموعة تعد كلمة سر قوية حسب المواصفات التالية :

- يجب ان تحتوي على حروف انجليزية
- يجب ان تكون طول الكلمة لا تقل عن ١٠ خانات
- يجب ان تحتوي على حروف صغيرة و حروف كبيرة
- يجب ان تحتوي على أرقام
- يجب ان تحتوي على رموز مثل # @ &) (

كلمة السر هي: .....

تخمين كلمات السر لشبكة الواي فاي

نشاط ٢

الآن نختبر قوة كلمات المرور لكل مجموعة

https://haveibeenpwned.com/

عناصر و أهداف
الجلسة التدريبية الثانية

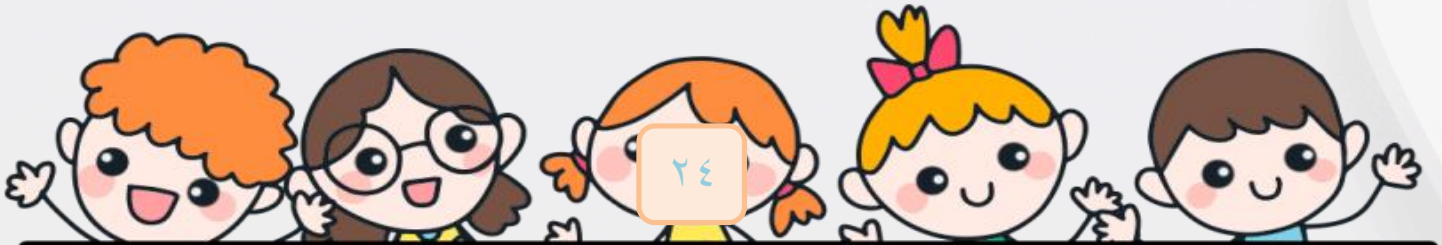
عناصر الجلسة:

- كيف نحمي بياناتنا في:
  ١. شبكات الواي فاي العامة.
  ٢. من خطر برمجيات الدعاية و الإعلانات.
  ٣. تقنية البلوتوث.
- نظام مكافحة الجرائم المعلوماتية.

أهداف الجلسة:

يتوقع في نهاية الجلسة أن تكون الطفل قادراً على:

١. أن تحمي نفسك في الشبكات اللاسلكية العامة.
٢. ان تعرف برمجيات الدعاية و الإعلانات وكيفية الوقاية منها.
٣. أن تعرف كيف تحمي نفسك في تقنيات البلوتوث.
٤. ان تعرف أن هناك قانون يحميه في حال تعرض للانتحال وهو قانون الجرائم الالكترونية.



المادة العلمية للجلسة الثانية

حماية الهوية الالكترونية

طرق الحفاظ على هوياتنا الالكترونية في كلاً من

الشبكات اللاسلكية العامة

Wifi

من خطر برمجيات الدعاية و الاعلانات

تقنية البلوتوث

الشبكات اللاسلكية العامة

تسمح الشبكات اللاسلكية و المعتمدة على تقنية الواي فاي للأجهزة اللوحية و المحمولة بالاتصال بالشبكة و الاستفادة من خدمة الانترنت

توجد غالباً في المطارات و المولات و الحدائق العامة

لا تتصفح بياناتك الخاصة مثل البريد و البنك.

عدم تفعيل مشاركة البيانات.

تفعيل كلمة مرور و الرقم سري.

برمجيات الدعاية و الإعلان Adware

نقاش٣

ما رأيك في الدعاية و الإعلانات التي تظهر اثناء لعب لعبتك المفضلة و لماذا ؟

برمجيات الدعاية و الإعلان Adware

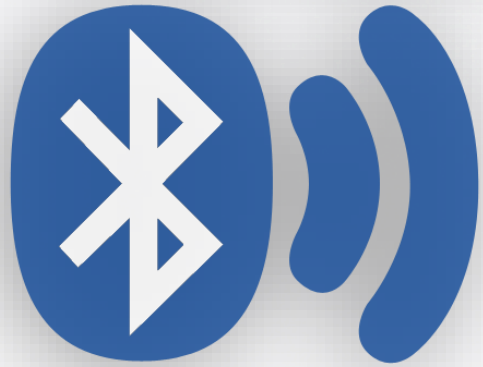
هي برمجيات صممت لإظهار إعلانات للمستخدمين دون رغبتهم في ذلك يتم تثبيته في حال تثبيت برامج أو العاب رديئة

الغرض منها

بعضها يتخصص في اظهار الإعلانات الا أن الكثير منها يهدف إلى التجسس

احذف أي لعبة الكترونية تكثر فيها الإعلانات
لا تستجيب للإعلانات سواء التي تظهر اثناء تصفح الانترنت او مع الألعاب.

تقنية البلوتوث Bluetooth



تقنية البلوتوث Bluetooth

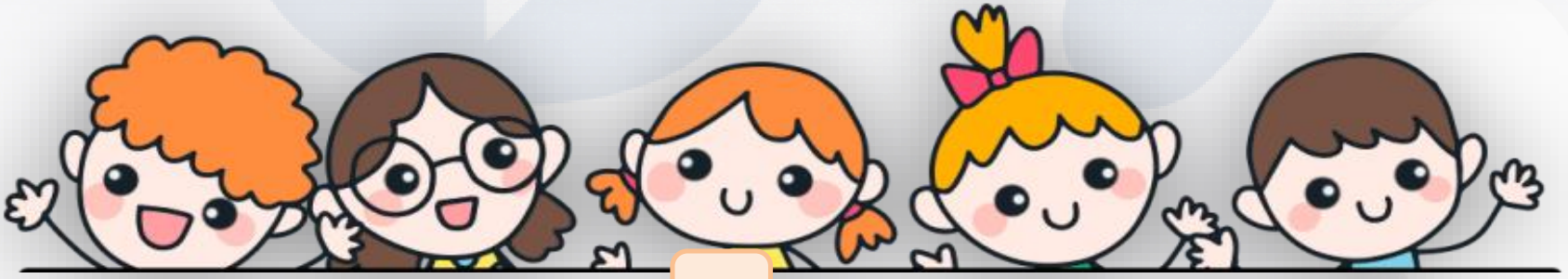
تقنية البلوتوث : هي تقنية تسمح بالتواصل فيما بين الأجهزة و نقل ومشاركة الملفات

للأسف يمكن للمخترقين أن يتمكنوا منه بسهوله سواء:

- التنصت
- التحكم عن بعد
- تثبيت برمجيات خبيثة
- استنزاف البطارية.

لتجنب كل ذلك بسهولة

قم بغلق البلوتوث في حال عدم استخدامه.



نشاط ٣

مراجعة لما سبق ؟

طرق سرقة الهوية الالكترونية

برمجيات الدعاية و الإعلان Adware

الهوية الإلكترونية

لا تخاف ولا تتردد بأن تخبر والديك بأي نشاط مختلف على أجهزتك الالكترونية .

وتذكر دائماً أن هناك نظام يحمي حقك بعد حماية الله وهو نظام مكافحة الجرائم المعلوماتية.

https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf

حفظكم الله من كل شر

انتهى دليل المتدرب

العرضِ المرئي

حماية الهوية الالكترونية

بقيادة المدرب:.....

١٤٤١هـ

الهوية الالكترونية

المعلومات الشخصية

- الهوية الحقيقية
- الهوية الإلكترونية

الهوية الحقيقية

هي التي يعرفك بها عائلتك و اصدقائك في المحيط الذي تعيش فيه مثل عمرك و عنوانك الحقيقي

الهوية الإلكترونية

هي التي تدخل بها الى العالم الرقمي و التي تظهر بها للآخرين على شبكة الانترنت و يفترض ان تكون قليلة للغاية .

نقاش

ما رأيك في مشاركة موقعك في برنامج السناب شات
أو الإنستغرام و لماذا ؟

كيف نحمي بياناتنا و خصوصيتنا في مواقع التواصل الاجتماعي

SOCIAL MEDIA ICONS

في شبكات التواصل الاجتماعي

- لا تشارك إلا بالقليل من المعلومات .
- لا تكمل ملفك الشخصي على مواقع التواصل الاجتماعي و قم بإعطاء أقل معلومة ممكنة.
- تأكد أن من يطلع على انشطتك في شبكات التواصل هم فعلاً اصدقائك ومن تريد أن يتابعونك.

نشاط ١

بشكل فردي :خلال دقيقتين :

اذكري شبكات التواصل الاجتماعي التي تفضلينها ؟

ماهي المعلومات الشخصية التي تشاركينها متابعيك ؟

SOCIAL MEDIA ICONS

نقاش ٢

ماذا يريد المهاجمون منك ؟

طرق سرقة الهوية الالكترونية

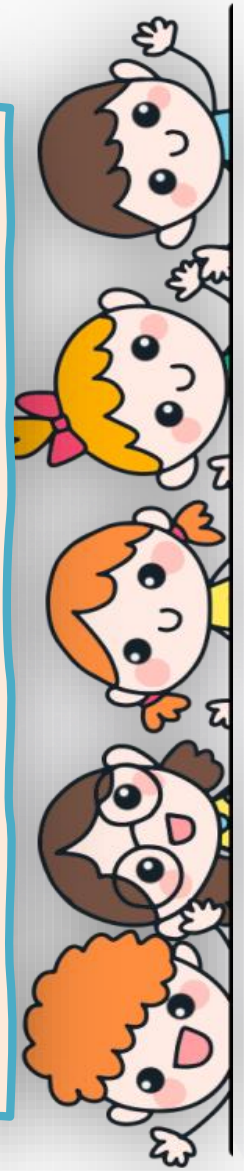
- الهندسة الاجتماعية
- استغلال الثغرات
- تخمين كلمات السر لشبكة الواي فاي
- الخداع

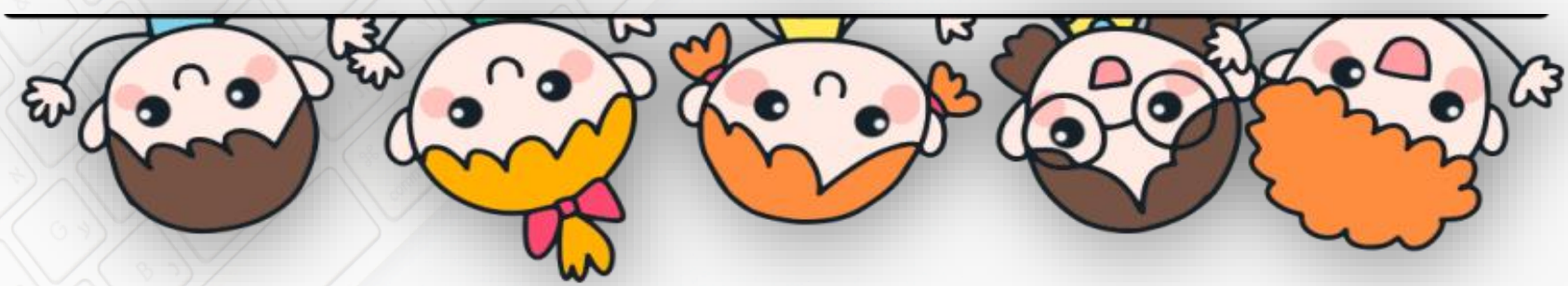
الهندسة الاجتماعية

هي الطرق الاجتماعية المختلفة للوصول الى الشخص و إقناعه في تنفيذ فعل ما أو الادلاء بمعلومات سرية

طرق الهندسة الاجتماعية

- الكذب و الخداع لسرقة كلمات سرية
- تتبع الاشخاص ومحاولة الدخول معهم في الانظمة
- شيء مقابل شيء





الخداع :

يرسل المهاجم رسالة على انها من مصدر موثوق و الرسالة تقنع المستخدم بمشاركة معلوماته المالية أو تثبيت برنامج خبيث

أحذر أن

- تفتح أي مرفق في البريد الالكتروني او رسالة سواء نصية أو واتس الا اذا كان المرسل معروف لديك
- تستجيب لأي رسالة طلب اذا لم تفهم معناها و أخبر أحد والديك
- ترسل بياناتك الشخصية و بيانات البطاقات البنكية .

تخمين كلمات السر لشبكات الواي فاي

يجب أن تحتوي جميع أجهزتنا على كلمات سر قوية حتى لا يستطيع المتطفل تخمين كلمات السر ثم الوصول على بياناتنا الشخصية

تخمين كلمات السر لشبكة الواي فاي

نشاط ٢

خلال دقيقة كل مجموعة تعد كلمة سر قوية حسب المواصفات التالية :

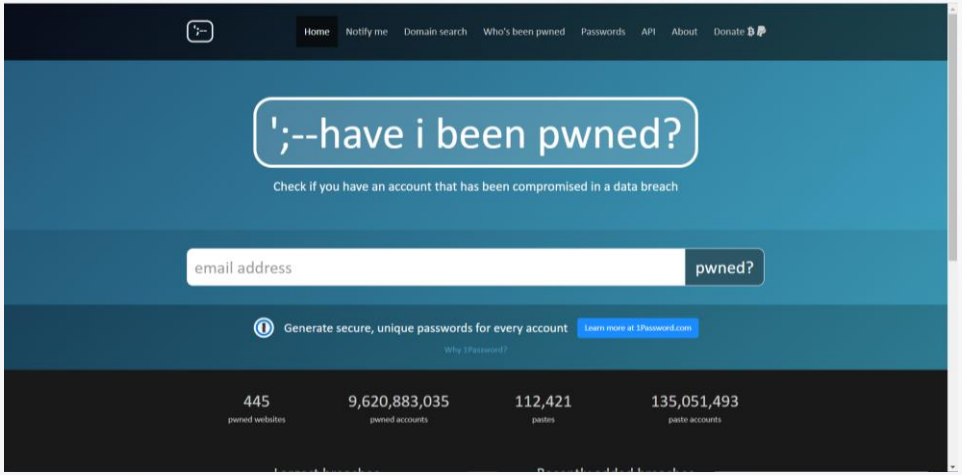
- يجب ان تحتوي على حروف انجليزية
- يجب ان تكون طول الكلمة لا تقل عن ١٠ خانات
- يجب ان تحتوي على حروف صغيرة و حروف كبيرة
- يجب ان تحتوي على أرقام
- يجب ان تحتوي على رموز مثل # @ &) (

تخمين كلمات السر لشبكة الواي فاي

نشاط ٢

الآن نختبر قوة كلمات المرور لكل مجموعة

https://haveibeenpwned.com/



وقت الراحة

حماية الهوية الالكترونية

بقيادة المدربة : م.منى الثويعي

طرق الحفاظ على هوياتنا الالكترونية في كلاً من

الشبكات اللاسلكية العامة

Wifi

من خطر برمجيات الدعاية و الاعلانات

تقنية البلوتوث

الشبكات اللاسلكية العامة

تسمح الشبكات اللاسلكية و المعتمدة على تقنية الواي فاي للأجهزة اللوحية و المحمولة بالاتصال بالشبكة و الاستفادة من خدمة الانترنت

توجد غالباً في المطارات و المولات و الحدائق العامة

لا تتصفح بياناتك الخاصة مثل البريد و البنك.

عدم تفعيل مشاركة البيانات.

تفعيل كلمة مرور و الرقم سري.

برمجيات الدعاية و الإعلان Adware

نقاش٣

ما رأيك في الدعاية و الإعلانات التي تظهر اثناء لعب لعبتك المفضلة و لماذا ؟

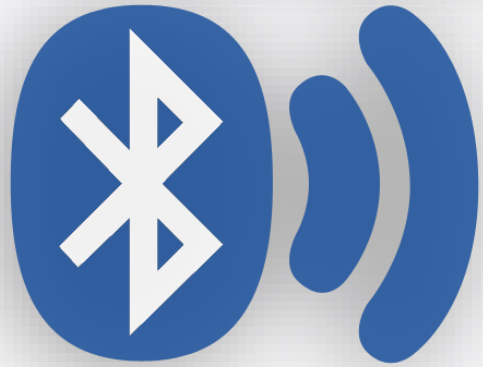
هي برمجيات صممت لإظهار إعلانات للمستخدمين دون رغبتهم في ذلك
يتم تثبيته في حال تثبيت برامج أو العاب رديئة

الغرض منها

بعضها يتخصص في اظهار الإعلانات الا أن الكثير منها يهدف إلى التجسس

احذف أي لعبة الكترونية تكثر فيها الإعلانات
لا تستجيب للإعلانات سواء التي تظهر اثناء تصفح الانترنت او مع الألعاب.

تقنية البلوتوث Bluetooth



تقنية البلوتوث Bluetooth

تقنية البلوتوث : هي تقنية تسمح بالتواصل فيما بين الأجهزة و نقل ومشاركة الملفات

للأسف يمكن للمخترقين أن يتمكنوا منه بسهوله سواء:

- التنصت
- التحكم عن بعد
- تثبيت برمجيات خبيثة
- استنزاف البطارية.

لتجنب كل ذلك بسهولة

قم بغلق البلوتوث في حال عدم استخدامه.

نشاط ٣

مراجعة لما سبق ؟

طرق سرقة الهوية الالكترونية

برمجيات الدعاية و الإعلان Adware

الهوية الإلكترونية

لا تخاف ولا تتردد بأن تخبر والديك بأي نشاط مختلف على أجهزتك الالكترونية .

وتذكر دائماً أن هناك نظام يحمي حقك بعد حماية الله وهو نظام مكافحة الجرائم المعلوماتية.

https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf

حفظكم الله من كل شر

انتهى البرنامج التدريبي