حماية
Hemaya

نبذة عامة عن
المجموعة السعودية لأمن المعلومات

آخر تحديث: ٢٠١٨/٩/١

@HemayaGroup

www.HemayaGroup.org

تصميم: ندى العي | أبرار الرفاعي

محتويات التقرير

مجموعة حماية

هي مجموعة سعودية تطوعية تحوي عدد يتجاوز المئتين عضوًا سعوديًا مختصًا بمجال أمن المعلومات، وبتنوع يغطي كافة تفرعات المجال التقنية والإدارية والاجتماعية والإنسانية. تسعى المجموعة إلى المساهمة بنهضة وطنها وتحقيق رؤيته وذلك بالمبادرة بتقديم خبرات أعضائها مجانًا في كل ما من شأنه تعزيز الوعي للمجتمع والكفاءة للمختص بمجال أمن المعلومات وفق المسار التالي:

الرؤية

أن تكون المجموعة مرجعاً في أمن المعلومات بالمملكة لِتُسهم في الارتقاء بواقع المجال.

الرسالة

رفع مستوى ثقافة أمن المعلومات والخصوصية وتعزيز المحتوى العربي من قبل مختصين سعوديين.

المبادئ

١. مجموعة حماية لا تخرج عن سياسات حكومة خادم الحرمين الشريفين وأنظمة المملكة العربية السعودية وتدين بالولاء والسمع والطاعة لها.

٢. أعضاء حماية معروفون بأسمائهم الصريحة و لا نقبل ولا نتعامل مع أي شخصية لاتصرح باسمها.

٣. مجموعة حماية لا تقوم ولا تعلم ولا تؤيد أي أعمال اختراق تحت أي مسمى كان.

٤. مجموعة حماية تقدر جميع الجهود التي تبذل في سبيل أمن المعلومات في المملكة العربية السعودية و عليه فإنها تدعو دائماً للتطوير و تسعى لطلب الأفضل كجهود مكملة وداعمة.

الأهداف

- نشر مفهوم أمن المعلومات بقالب صحيح متوازن يُسهم في زيادة الثقافة والمعرفة العلمية.
- بناء قاعدة معلومات باللغة العربية خاصة في مجال أمن المعلومات ومختصيها.
- دعم المجتمع وطلبة الجامعات معلوماتياً فيما يخص مجال أمن المعلومات.
- تشجيع المختصين والباحثين على المشاركة في الأبحاث المتخصصة وكتابة التقارير والمقالات الدورية التي تسهم في تطوير واقع أمن المعلومات.
- توفير حلقة وصل بين حماية والجهات الحكومية في سبيل التطوير ونقل المعرفة.
- تقديم محتوى توعوي في أمن المعلومات.

مجالات الإختصاص

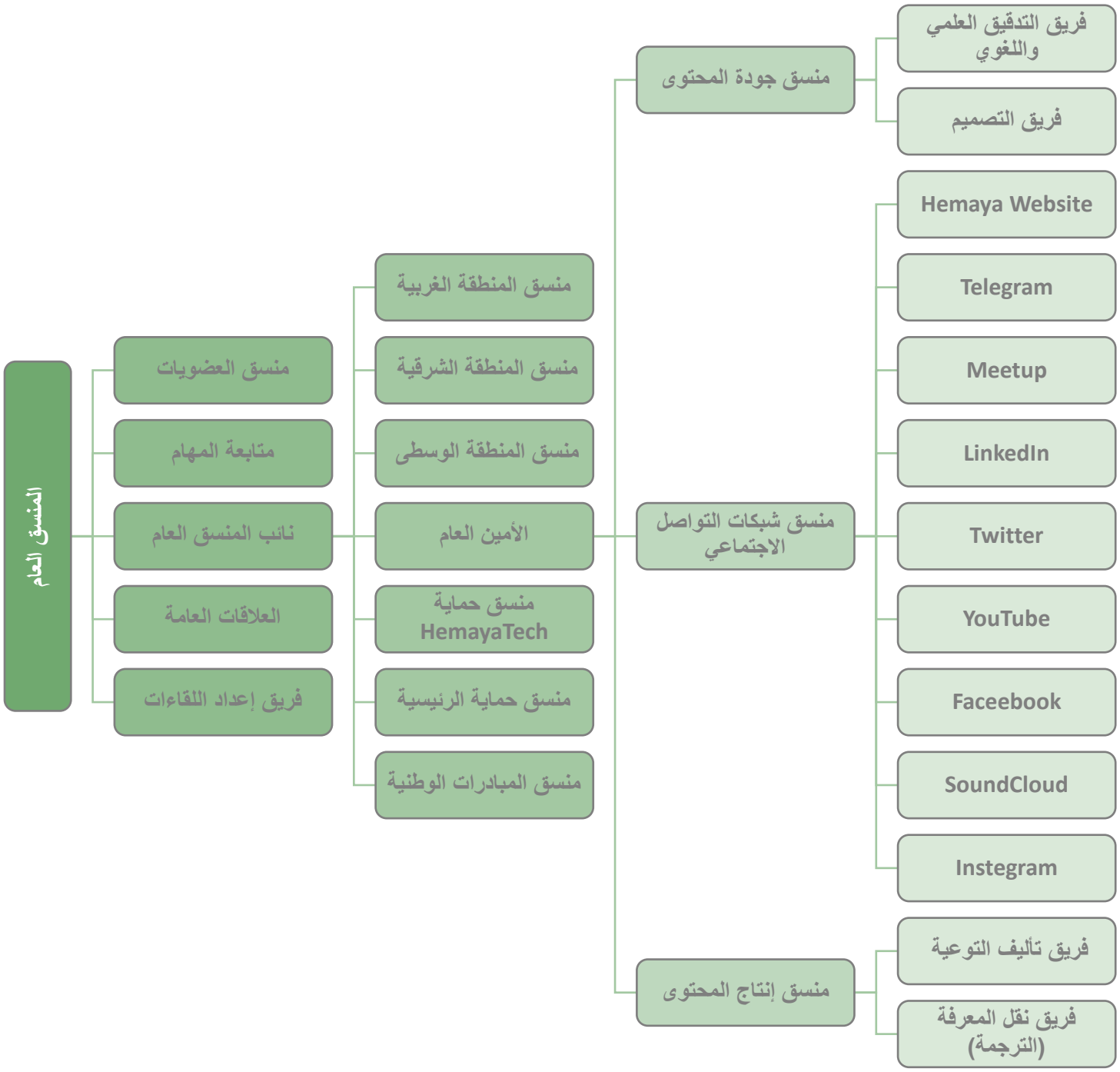
- تقنيات أمن المعلومات
- أمن البرامج والتطبيقات
- أمن الشبكات والإتصالات
- الجرائم المعلوماتية والتحقيق الرقمي الجنائي
- إدارة أمن المعلومات والخصوصية
- أمن نظم التشغيل والأجهزة الذكية

www.HemayaGroup.org

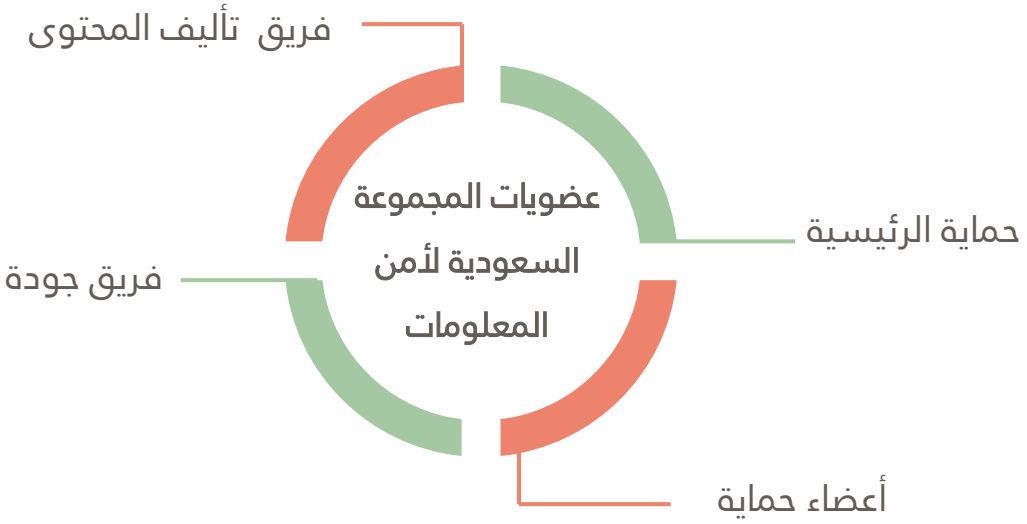
Saudi Group for Information Assurance - المجموعة السعودية لأمن المعلومات - حماية


122 فيديو
50 منشورات (انفوجرافيك)
11 بودكاست ساوند كلاود
5 نصائح مصوره
كن محمي
تشفير على السريع
امان مواقع التواصل الاجتماعي
الهوني بوت (HoneyPot)
التحقيق الجنائي الرقمي
الهندسة الاجتماعية
محتويات أمن المعلومات
كتيب دليل المستخدم لأمن المعلومات
450 عضو مختص في أمن المعلومات
حقيبة المعلم التوعوية بأمن المعلومات لطلاب المدارس العامة
أبحاث علمية
المشاركات المجتمعية
أعمال مجموعة حماية
أكثر من 25 مشاركة مجتمعية متنوعة مابين ورش عمل ومحاضرات ومشاركات اعلامية
2 لقاء حواري
المبادرات الوطنية
عدد المتابعين في شبكات التواصل الإجتماعي أكثر من 19K متابع
7 محاضرات أكاديمية
11 محاضرة تقنية
توصيات في الأمن المعلوماتي للتعامل مع تهديدات الهجمات الإلكترونية للمؤسسات
التوصية بدعم شهادات مهنية لأمن المعلومات ضمن برنامج هدف لتمنية الموارد البشرية
توصية للمركز الوطني لدعم أمن المعلومات للمؤسسات الصغيرة والمتوسطة بالمملكة
www.hemayagroup.org
@HemayaGroup
المجموعة السعودية لأمن المعلومات
28/8/2018
تصميم: سماهر العرابي
@i_smaher

• الهيكل الإداري لمجموعة حماية



• أعضاء مجموعة حماية



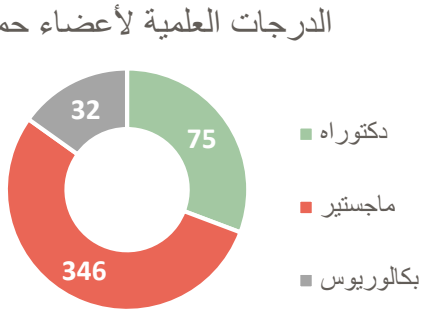
○ أعضاء حماية الرئيسية

تتميز هذه المجموعة بالتنوع المعرفي والعلمي والخبرات المتراكمة لأعضائها في كافة مجالات أمن المعلومات الدقيقة والمشتركة مع الإختصاصات الأخرى. تمتاز محاضراتها بالبعد الاستراتيجي للأمن الإلكتروني والإكاديمي والبحثي. هذه المجموعة تعتبر نواة حماية والمجموعة الرئيسية لكيانها. أعضاء هذه المجموعة من الجنسين وتعقد أنشطتها في مدينة الرياض وجدة (وقريبًا في الدمام). يقبل في عضوية هذه المجموعة المتخصيين السعوديين في مجال أمن المعلومات فقط. قبل الإنضمام للمجموعة يجب أن يكون العضو عضوًا في حماية التطبيقة ويساهم في خدمة المجتمع أو أحد أنشطة المجموعة.

○ أعضاء حماية التقنية

تتميز هذه المجموعة بالتنوع المعرفي العملي التطبيقي. تركز في كافة أنشطتها على التحديات اليومية لأمن المعلومات والحلول الفورية لها. تمتاز محاضراتها بالتركيز على الجانب العملي للأمن الإلكتروني. هذه المجموعة تعتبر رافد أساسي للمجموعة الرئيسية. أعضاء المجموعة من الجنسين وتعقد أنشطتها في مدينة الرياض . يقبل في عضوية هذه المجموعة المتخصيين السعوديين في

مجال أمن المعلومات فقط وتتشرف بحضور الأشقاء العرب في لقاءاتها. للانضمام تواصل معنا عبر حسابنا في تويتر.

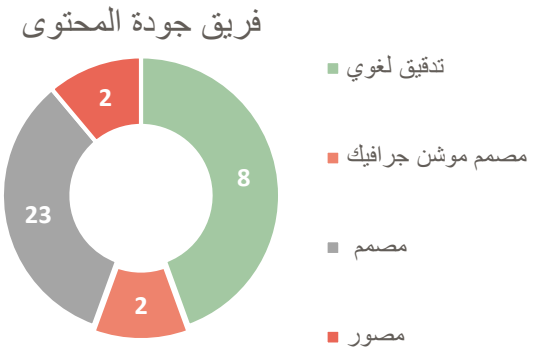


- **فريق تأليف المحتوى**

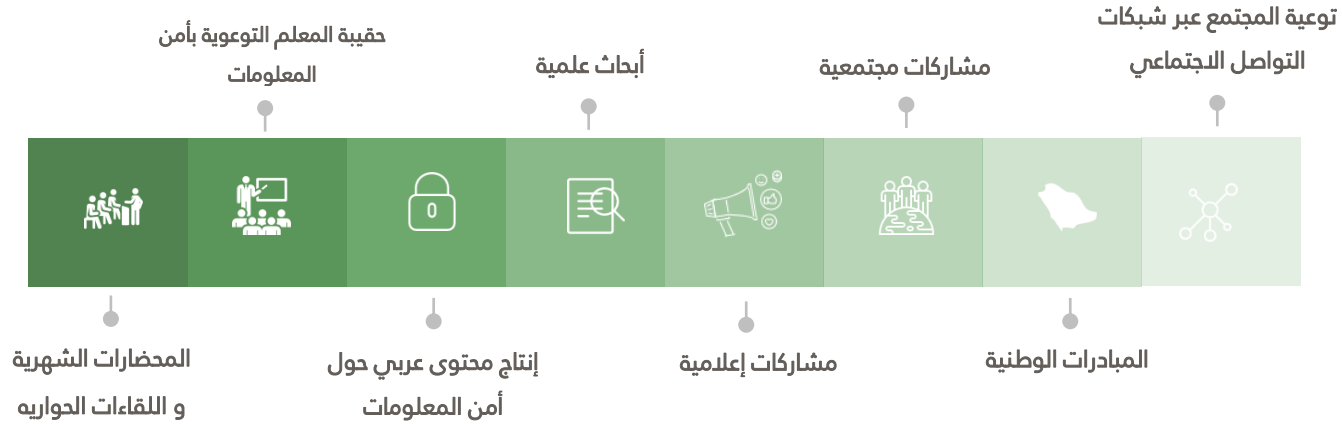
هو فريق معني بتاليف المحتوى التوعوي و تدقيق المعلومات المقدمة وتبسيطها لأقصى قدر ممكن لتيسير فهمها من عامة المجتمع. أعضاء الفريق هم أعضاء في حماية الرئيسية أو حماية التقنية.

- **فريق جودة المحتوى**

يتميز هذا الفريق بتنوع مهاراته وإمكانياته التي يسخرها في خدمة المجموعة والمجتمع. ويتنوع ما بين مصممين و مدققين لغويين و تربويين تتركز وظيفتهم في مراجعة وضبط المحتوى المقدم من المجموعة وإخراجها ومراجعته قبل النشر. أعضاء الفريق من الجنسين ويقوم بأعماله عبر شبكات التواصل الاجتماعي. يقبل في عضوية هذا الفريق من كان مختصًا باللغة العربية أو مصمم (فوتوشوب، انفوجرافيك، فيديو، موشن جرافيك) أو أي مهارة تعتقد إنك تستطيع دعم المجموعة بها . للإنضمام تواصل معنا عبر حسابنا في تويتر .



• أهم أنشطة مجموعة حماية



○ توعية المجتمع عبر شبكات التواصل الاجتماعي

جميع ما ينشر هو لإثراء المحتوى العملي في أمن المعلومات، ولنشر ثقافة وممارسات أمن المعلومات، ولتقديم محتوى توعوي في أمن المعلومات باللغة العربية.

الموقع الإلكتروني	http://hemayagroup.org
حساب التويتر	@HemayaGroup
قناة مرئية (YouTube)	HemayaGroup
قناة صوتية (Soundcloud)	HemayaGroup
Telegram	HemayaGroup
Meetup	HemayaGroup
Facebook	HemayaGroup
Instagram	HemayaGroup

المبادرات الوطنية

- مبادرة في الأمن المعلوماتي للتعامل مع تهديدات الهجمات الإلكترونية للمؤسسات - السياسات الأساسية لضمان بيئة آمنة. أعدها مجموعة من الأعضاء و قدمت لعضو مجلس الشورى أستاذ دكتور جبريل العريشي.
- مبادرة للمركز الوطني لدعم أمن المعلومات للمؤسسات الصغيرة والمتوسطة بالمملكة. أعدها مجموعة من الأعضاء و قدمت لعضو مجلس الشورى أستاذ دكتور جبريل العريشي وأرسلت لمجلس الشؤون الاقتصادية والتنمية.
- مبادرة بدعم شهادات مهنية لأمن المعلومات ضمن برنامج هدف لتمنية الموارد البشرية. أعدها مجموعة من الأعضاء وقدمت للدكتور عبدالعزيز السعيد لتسليمها لمسوؤلي برنامج هدف.

مشاركات مجتمعية

- شاركت حماية بورش عمل للدكتوره سعاد العريفي و للأستاذ فهد الشمران و للأستاذ عبدالله القحطاني بالبرنامج الاثرائي في ملتقى الرياض الاجتماعي الثالث المنعقد يوم الاثنين ٢٦ جماد اللآخر ١٤٣٧ الموافق ٤ أبريل ٢٠١٦. قدمت د.سعاد ورشة عمل بعنوان المراءه ووسائل التواصل الاجتماعي. وقدم الأستاذ فهد الشمران و الأستاذ عبدالله القحطاني ورشة عمل بعنوان الامن المعلوماتي.
- استضاف نادي تقنية المستقبل بجامعة الملك سعود المهندس علي الشهري في يوميات موظف أمن معلومات الثلاثاء ١ صفر ١٤٣٨ الموافق ١ نوفمبر ٢٠١٦. حيث قدم المهندس محاضره عن أمن المعلومات من منظور الوظيفة العملية.
- شاركت حماية بمحاضرة للأستاذ وائل فتوح وايضا بورش عمل للأستاذ وائل فتوح و للأستاذ محمد العصيمي ضمن المؤتمر الخامس للمراجعة الداخلية (٢٢-٢٤ صفر ١٤٣٨ الموافق ٢٢-٢٤ نوفمبر ٢٠١٦) برعاية الجمعية السعودية للمراجعين الداخليين.
- شاركت مجموعة حماية في حملة "أمانكم" التوعوية التي انطلقت ٦ صفر ١٤٣٨ هـ الموافق ٦ نوفمبر ٢٠١٦ عبر شبكات التواصل الأجتماعي برعاية مجموعة كونوا بخير الوطنية واختتمت ٢١ ربيع الاخر ١٤٣٨ هـ الموافق ١٩ يناير ٢٠١٧.

- استضافت الجمعية السعودية للمراجعين الداخليين الأستاذ وائل فتوح يوم الثلاثاء ٢٤ جماد أول ١٤٣٨ الموافق ٢١ فبراير ٢٠١٧. حيث قدم الأستاذ ورشة عمل بعنوان الهجمات الإلكترونية ودور المراجع الداخلي.
- شاركت مجموعة حماية بورشة عمل عن أمن المنشئات الصغيرة والمتوسطة للدكتور ياسر هوساوي و الدكتورة سعاد العريفي و الدكتور جلال العوبيدي و الأستاذ زياد العبود ضمن المؤتمر الدولي الثاني للأمن الإلكتروني (٥/٣٠-٦/١ ١٤٣٨ الموافق ٢٧-٢٨ فبراير ٢٠١٧) برعاية مركز الأمن الإلكتروني.
- استضافت مجموعة هاويات التقنية السعوديات الأستاذ محمد المزين يوم الثلاثاء ٨ جماد الاخر ١٤٣٨ الموافق ٧ مارس ٢٠١٧. حيث قدم الأستاذ محاضرة بعنوان خارطة طريقك في مجال أمن المعلومات.
- شارك مؤسس مجموعة حماية الاستاذ متعب الضبيطي بمحاضرة عنوانها "أمن المعلومات...حياتياً و أكاديمياً و مهنيا"" ضمن اللقاء الالكتروني الأول للمتعثين (١٠-١٢ رجب ١٤٣٨ الموافق ٧-٩ ابريل ٢٠١٧) الذي كان برعاية مجموعة انطلق للبعثة.
- في مجال دعم طلاب الجامعات شاركت حماية بمراجعة انفوجرافيك لطالبات في قسم تقنية المعلومات في كلية علوم الحاسب و المعلومات في جامعة الملك سعود. كانت هذي الانفوجرافيك عباره عن مشاركة في خدمة المجتمع من الطالبات في التوعية بموضوع "Cloud Storage"و "Spear Phishing" و "هجمات شمعون."
- قدم المهندس علي الشهري محاضرة بعنوان "الاستخدام الآمن للأجهزة الذكية و وسائل التواصل الاجتماعي" في فعاليات برنامج غير جوك الشبابي بتنومة السبت ١٢ ذو القعدة ١٤٣٨ الموافق ٥ أغسطس ٢٠١٧.
- استضافت كلية المجتمع في جامعة الأميرة نورة الأستاذ محمد المزين يوم الخميس ١٣ صفر ١٤٣٩ الموافق ٢ نوفمبر ٢٠١٧. حيث قدم الأستاذ محاضرة عبارة عن مدخل ميسّر لمجال أمن المعلومات. غطت المحاضرة مبادئ أمن المعلومات و نطاقات أمن المعلومات كما تم تسليط الضوء على المسارات المختلفة في هذا المجال.

- قدمت حماية بالتعاون مع سمعية (@shi_org_sa) محاضرتين توعويتين للصم وضعاف السمع قدمها المهندس علي الشهري و الدكتورة أريج الحقيل يوم السبت ٧ ربيع أول ١٤٣٩ هـ الموافق ٢٥ نوفمبر ٢٠١٧. حيث قدم م.علي محاضرة بعنوان"الاستخدام الآمن للاجهزة الذكية" (https://youtu.be/la5a3DGzunM) وقدمت د.أريج محاضرة بعنوان "آمن على الإنترنت.
- قدم المهندس علي الشهري محاضرة بعنوان "الاستخدام الآمن للأجهزة الذكية ووسائل التواصل الاجتماعي" في كلية التقنية بالنماص يوم الأحد ٢٨ ربيع أول ١٤٣٩ هـ الموافق ١٧ ديسمبر ٢٠١٧ م .وقد تحدث المهندس عن السلبيات والأيجابيات للأجهزة الذكية وكيف تصنع تصور الناس عنك في الفضاء الألكتروني وأخطاء المستخدمين العامة ونظرة عامة عن الجرائم الإلكترونية.
- قدمت الأستاذة اروى الحمد محاضرة لطالبات جامعة الأميرة نورة بعنوان :Cyber Crimes You are a Target" "يوم الخميس ٦-٦-١٤٣٩ هـ الموافق ٢٢-٢-٢٠١٨ م. وقد تحدثت الأستاذة عن تعريف الجرائم الإلكترونية و تاريخها و انواعها و كيفية التعامل معها مع ذكر بعض الإحصائيات و امثلة واقعية.
- قدم الأستاذ المثنى العقلا محاضرة بعنوان "الأمن الالكتروني: المخاطر والتحديات" وذلك في يوم الثلاثاء ٢٧ فبراير ٢٠١٨ في جامعة الأمير سلطان بالرياض كجزء من فعاليات يوم تقنية المعلومات .Smart Campus 2023 وتضمنت المحاضرة التعريف بتخصص أمن المعلومات ومساراته الاكاديمية والوظيفية، وأيضاً توعية عامة بكيفية التعامل مع الجرائم الإلكترونية.
- قدمت الأستاذة مها القريني محاضرة بعنوان "الجرائم المعلوماتية (وعيك سبيل آمنك)" وذلك في يوم الثلاثاء ١-٧-١٤٣٩ هـ الموافق ٢٧-٣-٢٠١٨ في جامعة الأميرة نورة بالرياض. غطت المحاضرة تاريخ الجريمة المعلوماتية وأقسامها وأنواعها والجهود الدولية لمواجهتها وبالأخص جهود المملكة العربيه السعوديه.

- استضافت كلية التقنية بالجوف الدكتور خالد العيسى و المهندس عمر العمر و المهندس مالك الدوسري و الأستاذة فايز الشمري كمتحدثين في ندوة "أمن المعلومات" التي أقيمت يوم الأربعاء ٢ شعبان ١٤٣٩ الموافق ١٨ أبريل ٢٠١٨. حيث قدموا معلومات قيمة وثرية حول الهجمات و الحروب و الجرائم الإلكترونية.
- شارك ٢٢ عضو من حماية كمحكمين و مرشدين في هاكاثون الحج لعام ٢٠١٨.
- استضافة إدارة برامج الشباب مساء يوم الأثنين ٦ أغسطس ٢٠١٨ الدكتور متعب الضبيطي و الأستاذ عبدالكريم البراهيمي في جلسة نقاش بعنوان (الاستخدام الآمن للتقنية).و تضمن النقاش التعريف بالتنمر وأسبابه ودوافعه والطرق المناسبة للحماية منه. وأيضاً تم التطرق لتأثير الألعاب الإلكترونية على الأطفال وكيفية الحماية منها، و على ضرورة الاهتمام بالأمن الشخصي الإلكتروني.

مشاركات إعلامية

- تحدث عضو المجموعة المهندس سعود الصويمل عن تطبيق كلنا أمن عبر برنامج مرايا ناعمة. (https://youtu.be/xfJnahDct9o).
- شارك الأستاذ أحمد الحصيني في القناة الثقافية السعودية في حديث عن شبكات التواصل الاجتماعي وطرق اختراقها وحمايتها (https://youtu.be/QlBhfiA1yys).
- تحدث عضو المجموعة د.حسين الجحدلي عن الجرائم الالكترونية في برنامج صباح السعودية (https://youtu.be/-jtHd6Gx23g).
- تحدثت عضوة المجموعة د.أريج الحقيل عن **اليوم العالمي لأنترنت آمن** في برنامج اكتيفيتي على إذاعةUFM

(https://www.youtube.com/watch?v=AlvJHU6xNWA&feature=youtu.be).
- شارك الدكتور ياسر هوساوي عبر برنامج "العين عليك" في قناة السعودية "العائلة" بلقاء توعوي حول التحقق الرقمي للهوية بهدف إكساب المشاهد الوعي حول مفهوم وأنواع التحقق الرقمي للهوية وأساليبه وآلياته والوسائل المستخدمة لإتمام عملية التحقق. وفِي اللقاء تم ذكر بعض النصائح والإرشادات التي من شأنها مساعدة المشاهدين في الحفاظ على المعرفات الشخصية التي تستخدم في عمليات التحقق، والتي بدورها ستسهم في الحفاظ على أمن المعلومات والخصوصية الرقمية في حال استخدامها بالشكل المطلوب.

https://www.youtube.com/watch?v=2DonxIcYNrY) ,

https://www.youtube.com/watch?v=s2fBuolD0lU

.(https://www.youtube.com/watch?v=ubxlAkUbTl0

- شارك الدكتور حسين الجحدلي عبر برنامج "العين عليك" في قناة السعودية "العائلة" بلقاء تلفزيوني تم فيه التطرق لماهية الجرائم المعلوماتية، و اقتصادياتها و من ذلك تسلسل الهجمات و كيفية ترابطها لينتج عنها مورد مالي مجزي. كما تم التعرض و شرح نظام مكافحة الجرائم المعلوماتية السعودي و أهم أهدافه.

(https://www.youtube.com/watch?v=_b-BH8rDDHw

https://www.youtube.com/watch?v=8VURUqlyamQ

.(https://www.youtube.com/watch?v=d5eKK8biqno

- شارك الدكتور حسين الجحدلي في لقاء تلفزيوني على القناة السعودية عبر برنامج "صباح السعودية" وكان اللقاء موجه لعامة المشاهدين لزيادة الوعي في عدة مجالات في امن المعلومات. من تطبيقات الجوال تم اختيار الواتساب كمنصة يتفاعل من خلالها ٧٠٠ مليون مشترك نشط، و بحجم ٣٠ مليار رسالة. و من الممارسات، تم التعريج على ممارسة حماية الطفل من قبل الوالدين فيما يخص الأجهزة الذكية و استخداماتها. كما تم التنويه عن أهمية تأمين الشبكات الداخلية لحماية الأجهزة الإلكترونية الذكية فيما يعرف بإنترنت الأشياء.

(https://www.youtube.com/watch?v=4iQRdM4ZCXI)

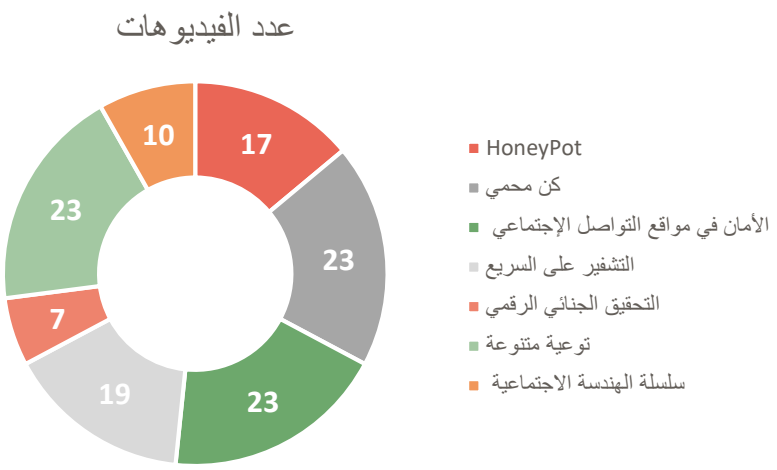
أبحاث علمية

- شارك ممثلي مجموعة حماية الدكتور سعد القحطاني و الأستاذة نورة القحطاني بنشر علمي محكم في المؤتمر الدولي الثاني للجرائم المعلوماتية المنعقد في جامعة الملك خالد (٢٧-٢٨ جماد الاخر ١٤٣٨ الموافق ٢٦-٢٧ مارس ٢٠١٧). حيث قدم الدكتور سعد ورقة علمية بعنوان-"A Forensic Acquisition Based upon A Cluster Analysis of Non Volatile Memory in IaaS" (للحصول على الورقة كاملة انقر هنا) ، والأستاذة نورة ورقة علمية بعنوان"A State of the Art Review of Internet Risks on Children" (للحصول على الورقة كاملة انقر هنا).

- شاركت الأستاذة نورة القحطاني بنشر علمي محكم في مؤتمر تقنيات وتطبيقات الإنترنت (Internet Technologies and Applications) المنعقد في دولة بريطانيا. حيث قدمت الأستاذة نورة ورقة علمية بعنوان "Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi Context" (للحصول على الورقة كاملة انقر هنا).

○ إنتاج محتوى بالعربي حول أمن المعلومات

- **المحتوى المرئي:**
  - سلسلة كن محمي (توعية تطبيقية علمية لتأمين أجهزة الحاسب الآلي وسلسة أخرى لتأمين شبكات التواصل الاجتماعي من (الألف إلى الياء) مجموعة من الفيدوهات التوعوية المنشورة على اليوتيوب.
  - سلسة الهوني بوت (HonePot): مجموعة حلقات موجهه للمحترفين .
  - سلسة الأمان في مواقع التواصل الإجتماعي : فيديوهات توعويه قصيرة للتوعية بالأخطار المحيطة لمستخدم شبكات التواصل الاجتماعي.
  - سلسة التشفير على السريع: فيديوهات تتكلم عن التشفير وتاريخه وأشهر الطرق في التشفير.
  - سلسلة التحقيق الجنائي الرقمي: مجموعة فيديوهات تتكلم عن ماهو التحقيق الجنائي الرقمي؟ و طرق التحقيق الجنائي الرقمي وغيرها من المسائل التي لها علاقة بالتحقيق الجنائي الرقمي.
  - سلسلة الهندسة الاجتماعية : هدف السلسله هو التوعية بمخاطر الهندسة الاجتماعية وعمليات الاحتيال.



- **المحتوى المقروء:**
  - كتيب دليل المستخدم لأمن المعلومات .
  - نصائح مصورة.
  - منشورات (انفوجرافك):
    - أخطر ١٠ ممارسات للموظفين
    - إرشادات لإنشاء كلمة مرور قوية
    - احم نفسك ضد الرسائل الغير موثوقة المصدر
    - التصفح الآمن
    - كيف تخترق الأجهزة الذكية؟
    - نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية
    - كيف تبلغ عن السب و الشتم عبر وسائل تقنية المعلومات؟
    - ماهو فيروس طلب الفدية؟ ماهي طرق الحماية منه؟
    - نصائح أمنية لإدارة حسابات الشبكات الاجتماعية للجهات الرسمية
    - كيف تبلغ عن الابتزاز الإلكتروني؟
    - تشفير تطبيق الواتساب
    - نبذة عن علم أمن المعلومات
    - حماية الشبكة الاسلكية

- نصائح عند الشراء من المواقع الإلكترونية
- كيف تحفظ مليون كلمة مرور بسهولة؟!
- أساليب الهندسة الاجتماعية
- نصائح توعوية للوالدين في كيفية متابعة أبنائهم في الألعاب الإلكترونية و الشبكات الاجتماعية
- التجسس الإلكتروني
- استخدام الحوسبة السحابية بأمان
- خطوات التعامل مع العصابات الدولية للابتزاز الإلكتروني
- لماذا يقال: إن الحلقة الأضعف في أمن المعلومات هم البشر!!
- ماذا تفعل لو وجدت محفظة مفقودة؟!
- الإنترنت بالسفر
- مخاطر استخدام مواقع التورنت لتحميل و مشاركة الملفات.
- خطوات تأمين الأجهزة الذكية (أندرويد و أبل).
- مصطلحات في الهجمات الإلكترونية.
- مصطلحات في البرمجيات الخبيثة.
- الخصوصية .. توضيحات ونصائح.
- مفاهيم مغلوطة في بروتوكول HTTPS.
- نقاط مهمة للحفاظ على الخصوصية الرقمية للمنظمات من قبل موظفيها.
- الأمان والخصوصية في حسابات توتير.
- عناصر التحكم الرئيسية لحماية المؤسسات.
- ماهو الأمن السيبراني؟
- الأدلة الرقمية.
- مبروك! لقد فزت بجائزة!
- أمن انظمة التحكم الصناعي SCADA.
- انواع التشفير.
- تسميم DNS.

- نظام عقوبات نشر الوثائق و المعلومات السرية و إفشائها.
- منع تسريب البيانات خارج المنظمة.
- الأستثمار الزائف.
- من هو المخترق الداخلي؟
- كيف تحمي حساباتك من الاختراق؟
- التحقق من الهوية.
- أفضل مؤتمرات الأمن السبراني.
- الاستخدام الأمثل للإنترنت.

○ حقيبة المعلم التوعوية بأمن المعلومات – طلاب المدارس العامة

جاري تعاون مع وزارة التعليم لإعداد و تطبيق حقائب توعوية بامن المعلومات لمراحل التعليم العام و رياض الأطفال . وكذلك تدريب من ترشحهم الوزارة على محتويات الحقائب و طرق توصيلها للفئة المستهدفة من الطلاب و الطالبات. **وتحوي الحقيبة على:**

- عرض باوربونت للتعريف بأمن المعلومات
- عشرين نصيحة معرفية كمطبوعات
- ستة شروحات فيديو توعوية لطرق تأمين شبكات التواصل الاجتماعي – تويتر، سناب شات، بريد الجيميل، بريد الهوتميل انستغرام، طرق كتابة الباسبورد.

○ اللقاءات الحوارية

- باستضافه من اكاديمية STC عقدت المجموعة السعودية لأمن المعلومات – حماية- لقاءها الحوراي بعنوان "قراءة نظامية للجريمة المعلوماتية والأدلة الرقمية في المملكة العربية السعودية" قدمها المحامي والمستشاري القانوني : عبدالله المحيميد وقد حضرها نخبة من المختصين ذوي الخبره الجنائية الرقمية والتقنية والقانونية قدموا مداخلات متنوعة تراعي اكثر من قراءه لموضوع الدليل الرقمي والأنظمة الخاصة بالجريمة المعلوماتية حسب وجهات النظر المختلفه حسب خبراتهم .

- أقامت المجموعة السعودية لأمن المعلومات – حماية- لقاء حواري بعنوان " نظام الخصوصية الأوروبي GDPR" قدمه الدكتور حازم المحيميدي استاذ بحث مساعد في المركز الوطني لتقنية أمن العلومات و ذلك في يوم السبت ٥ مايو ٢٠١٨ باستضافه من اكاديمية STC.

المحاضرات الشهرية لحماية

- تحديات أمن المعلومات في العالم العربي:

تاريخ اللقاء: الجمعة - ١٩ ربيع الأخر ١٤٣٧هـ الموافق ٢٩ يناير ٢٠١٦م

ضيف اللقاء : أ.د. جبريل العريشي – عضو مجلس الشورى سابقاً

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: www.youtube.com/watch?v=VAjaDicYPJI

صور من اللقاء:

- The Next Frontier of Security - Beyond Passive Denial and Isolation:

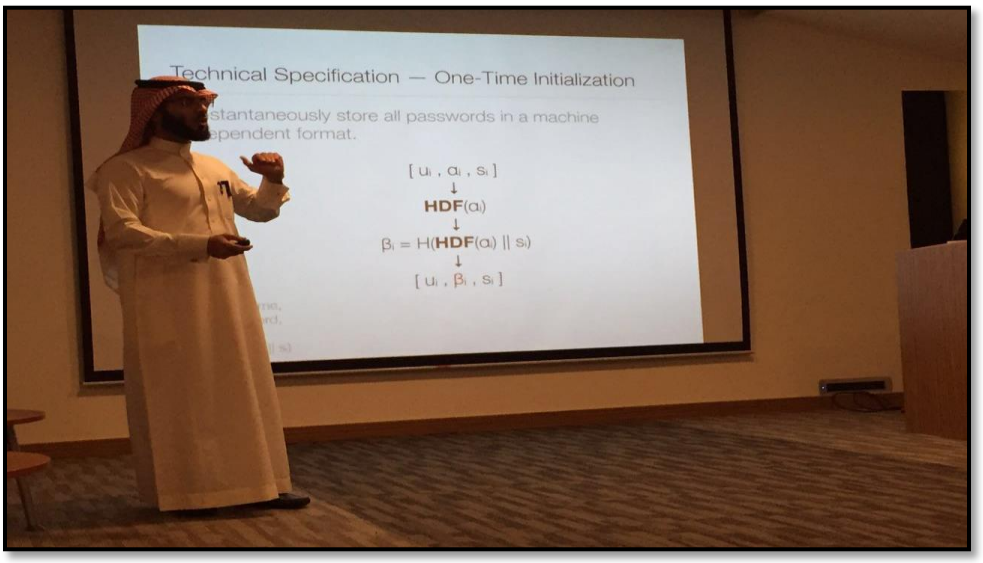
تاريخ اللقاء: الجمعة - ١٦ جماد الأخرة ١٤٣٧ هـ الموافق ٢٥ مارس ٢٠١٦م.

ضيف اللقاء : د. محمد المشيقح – استاذ مساعد - قسم نظم المعلومات - جامعة الملك سعود- رئيس مركز التميز سابقاً

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://youtu.be/Gd757VsUYlY

صور من اللقاء:



- هجمات تعطيل الخدمات الإلكترونية(DDoS) :

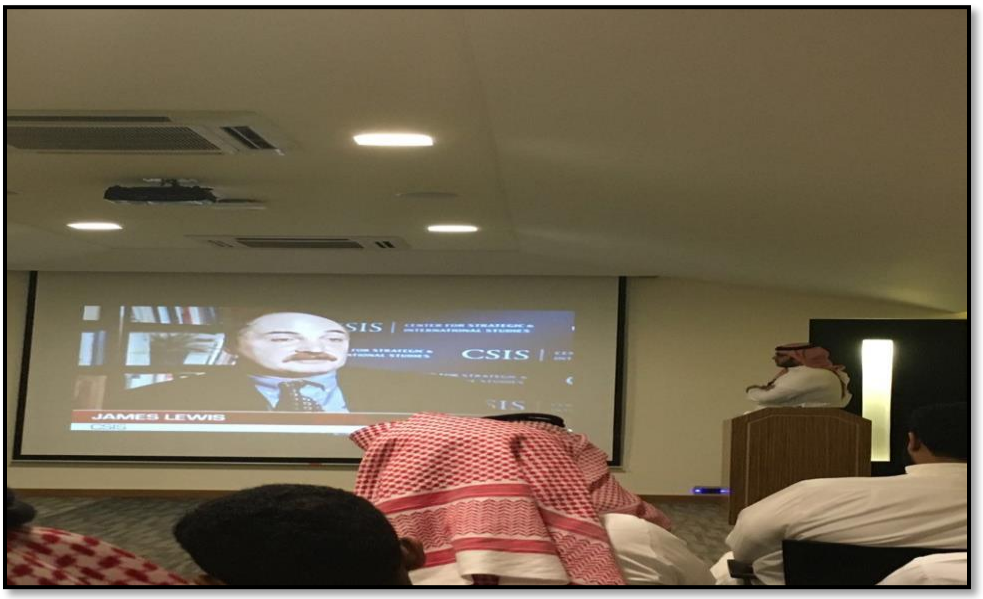
تاريخ اللقاء: الجمعة - ٢٢ رجب ١٤٣٧ هـ الموافق ٢٩ ابريل ٢٠١٦م.

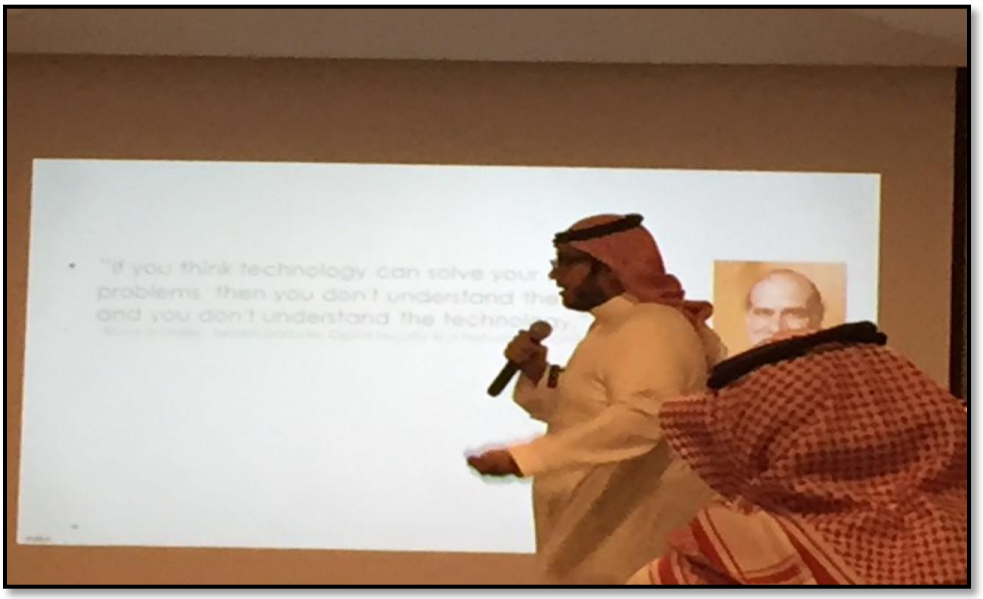
ضيف اللقاء: أ.المثنى العقلا – محلل حوادث أمن المعلومات

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://youtu.be/p5zkHYioqMQ

صور من اللقاء:





- Internet of Things: The Paradox of Private Identification:

تاريخ اللقاء: الجمعه - ٢٧ شعبان ١٤٣٧هـ الموافق ٣ يونيو ٢٠١٦م.

ضيف اللقاء : د. باسل العمير – مدير المركز الوطني لتقنيات أمن المعلومات – مدينة الملك عبدالعزيز للعلوم والتقنية

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://youtu.be/u-BG4Y5MpLM

صور من اللقاء:

- أساسيات مركز العمليات الأمنية (SOC) :

تاريخ اللقاء: السبت - ١٨ شوال ١٤٣٧ هـ الموافق ٢٣ يوليو ٢٠١٦ م.

ضيف اللقاء: أ.متعب الحربي

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://www.youtube.com/watch?v=FCvOOzLorb8

صور من اللقاء:

- أمن تطبيقات الويب:

تاريخ اللقاء: السبت - ١٠ ذو القعدة ١٤٣٧ هـ الموافق ١٣ اغسطس ٢٠١٦ م.

ضيف اللقاء: أ. محمد الدوسري

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://www.youtube.com/watch?v=xAlSD2IRQXI

صور من اللقاء:

- **التقنية و الاختراق الفكري:**

تاريخ اللقاء: السبت – ١ ذو الحجة ١٤٣٧هـ الموافق ٣ ستمبر ٢٠١٦م.

ضيف اللقاء : العقيد د. فهد الغفيلي ـ مدير إدارية المعلومات و الإنترنت بالإدارة العامة للأمن الفكري

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب

https://www.youtube.com/watch?v=b-V3exF0ZwU

صور من اللقاء:

- **التحليل الجنائي الرقمي في وحدة التخزين (USB) :**

تاريخ اللقاء: الخميس – ٥ محرم ١٤٣٨ هـ الموافق ٦ أكتوبر ٢٠١٦ م.

ضيف اللقاء : أ.د.دانيال الغزاوي -رئيس مجموعة أبحاث أمن المعلومات بجامعة الملك عبدالعزيز

موقع اللقاء: مقر أكاديمية دلة التطوعية – مدينة جدة

صور من اللقاء:

- **التعامل مع الحوادث الأمنية التقنية:**

تاريخ اللقاء: السبت - ٤ ربيع الأول ١٤٣٨ هـ الموافق ٣ ديسمبر ٢٠١٦م.

ضيف اللقاء: أ. سامي الأيداء

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

صور من اللقاء:

- **إدارة مخاطر تقنية المعلومات.:**

تاريخ اللقاء: السبت - ٢٥ ربيع الأول ١٤٣٨ هـ الموافق ٢٤ ديسمبر ٢٠١٦م.

ضيف اللقاء: أ. محمد العصيمي

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب

https://www.youtube.com/watch?v=Ayn4k1DV-i8

صور من اللقاء:

- **التخطيط لضمان استمرارية الأعمال:**

تاريخ اللقاء: السبت - ١٢ جماد ثاني ١٤٣٨ هـ الموافق ١١ مارس ٢٠١٧م

ضيف اللقاء: أ. ابو بكر آل سالم

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب :

https://www.youtube.com/watch?v=TpjGnYCx2Qc

صور من اللقاء:

- **السباق بين الرقابة وأنظمة تخطي الرقابة:**

تاريخ اللقاء: الخميس- ٣٠ رجب ١٤٣٨ هـ الموافق ٢٧ ابريل ٢٠١٧م

ضيف اللقاء: المهندس عبدالله القحطاني

موقع اللقاء: مقر أكاديمية دلة التطوعية – مدينة جدة

صور من اللقاء:

- **الكشف عن السلوكيات غير الاعتيادية من خلال تحليل حركة بيانات الشبكة باستخدام معالجة الإشارات العشوائية:**

تاريخ اللقاء: السبت - ٢٤ محرم ١٤٣٩ هـ الموافق ١٤ اكتوبر ٢٠١٧

ضيف اللقاء : د. باسل السدحان – أستاذ أمن الشبكات المساعد ومستشار أمن معلومات

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://www.youtube.com/watch?v=dhzEesHJEcw

صور من اللقاء:

- Introduction to Machine Learning: A Real Example in Cyber Security Field:

تاريخ اللقاء: السبت - ٨ صفر ١٤٣٩ هـ الموافق ٢٨ اكتوبر ٢٠١٧

ضيف اللقاء : م.ابراهيم الشمراني -مركز الأمن الالكتروني

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://youtu.be/nHVpDGacSAE

صور من اللقاء:

- Internet of Things: Opportunities and Security Challenges:

تاريخ اللقاء: السبت - ١٥ صفر ١٤٣٩ هـ الموافق ٤ نوفمبر ٢٠١٧.

ضيف اللقاء : الأستاذ مشعل العتيبي

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط اللقاء على موقع اليوتيوب: https://youtu.be/qwklBaSCZBw

صور من اللقاء:

- **التخطيط الاستراتيجي لأمن المعلومات في المنظمات:**

تاريخ اللقاء: الخميس - ١٩ ربيع أول ١٤٣٩ هـ الموافق ٧ ديسمبر ٢٠١٧.

ضيف اللقاء : د.هيا المقوشي

موقع اللقاء: غرفة جدة قاعة الشيخ صالح التركي – مدينة جدة

صور من اللقاء:

- أمن الحوسبة السحابية:

تاريخ اللقاء: السبت – ٢٧ ربيع أول ١٤٣٩ هـ الموافق ١٦ديسمبر ٢٠١٧.

ضيف اللقاء : أ. أروى الحمد

موقع اللقاء: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض.

رابط اللقاء على موقع اليوتيوب: https://www.youtube.com/watch?v=gXsj62oqUsQ

صور من اللقاء:

- أمن الهواتف الذكية:

تاريخ اللقاء: السبت – 5 شعبان ١٤٣٩ هـ الموافق ٢١ أبريل ٢٠١٨.

ضيف اللقاء : م. عبدالله العياضي

موقع اللقاء: الكلية التقنية بالدمام – مدينة الدمام.

صور من اللقاء:

- Threat Intelligence, Practically: A Walk through:

تاريخ اللقاء: الأثنين – ١٦ يوليو ٢٠١٨.

ضيف اللقاء : م. محمد المزين

موقع اللقاء: اكاديمية STC.– مدينة الرياض.

صور من اللقاء:

- ورش عمل
  - ورشة العمل الأولى:

تاريخ الورشة: يوم السبت ٢٥ رجب ١٤٣٨ هـ الموافق ٢٢ ابريل ٢٠١٧ م

ضيف الورشة: أ. عبدالرحمن النمري

موضوع الورشة: تطبيق عناصر التحكم الأساسية لحماية منشأتك (Top 20 Critical Security Controls)

موقع الورشة: مقر برنامج بادر لحاضنات التقنية (بادر) – مدينة الرياض

رابط الورشة على موقع اليوتيوب: https://www.youtube.com/watch?v=T9HfA3ZDGVs

صور من الورشة:

- ورشة العمل الثانية:

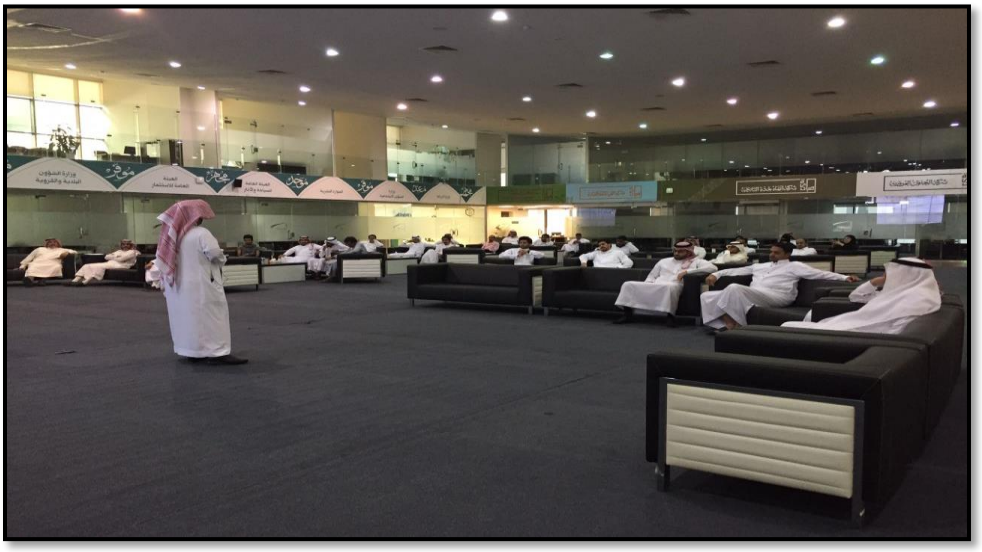
تاريخ الورشة: يوم السبت ٢١ شوال ١٤٣٨ هـ الموافق ١٥ يوليو ٢٠١٧ م

ضيف الورشة: أ. عبدالرحمن النمري

موضوع الورشة: تطبيق عناصر التحكم الأساسية لحماية منشأتك (Top 20 Critical Security Controls)

موقع الورشة: أكاديمية المصفق – مدينة جدة

صور من الورشة:



الملحق

مرفق عدد من منتجات حماية


أخطر 10 ممارسات للموظفين
الدخول على الشبكات اللاسلكية غير الآمنة
بقاء المعلومات السرية على الجهاز الشخصي
مشاركة كلمات المرور الشخصية مع الآخرين
استخدام(اسم مستخدم وكلمة مرور واحدة) لعدة حسابات
استخدام أجهزة تخزين خارجية غير مشفرة في تخزين معلومات حساسة ومهمة
ترك أجهزة الحاسب بدون رقابة خارج مكان العمل
عدم إبلاغ المنظمة عند فقدان جهاز تخزين خارجي يحوي معلومات سرية و حساسة
عدم استخدام حاجب الرؤية الجانبية على شاشة الجهاز عند التعامل عن بعد مع مستندات المنظمة السرية
حمل معلومات حساسة في الجهاز المحمول خلال السفر بدون ضرورة
استخدام أجهزة متنقلة شخصية للدخول على شبكة المنظمة
ترجمة فريق نقل المعرفة بمجموعة حماية
@HemayaGroup
المصدر Waffle Web Walk


كيف تُختَرق الأجهزة الذكية ؟
البرامج الخبيثة | Malware
أسهل الطرق للمخترقين, فالأدوات التي تصنع هذه البرامج الخبيثة متوافرة بكثرة في الإنترنت وكل ما على المخترق هو محاولة خداع المستخدم لتثبيت البرنامج على جهازه, كأن يرسل له رابط البرنامج الخبيث وإيهامه بأن هناك رسالة صوتية تركت له وبحثه على الضغط على الزر.
الهندسة الاجتماعية | Social Engineering
يقصد به خداع المستخدم البسيط واستغلال عدم درايته الكاملة بخدع و حيل المخترقين. على سبيل المثال يرسل المخترق رابط صفحة مزورة عبر البريد الإلكتروني وتكون مطابقة بشكلها العام الصفحة الأصلية للموقع ثم تطلب من الضحية إعادة تحديث بياناته ومن ثم تُرسل للمخترق.
FREE
Wi-Fi
الشبكات اللاسلكية المفتوحة | Open Wireless Networks
يستطيع المخترق باستخدام بعض أدوات التجسس بالتقاط بيانات المستخدم التي تنتقل ما بين جهازه وجهاز الوايرليس, لأن الشبكات اللاسلكية مجهولة المصدر أو الشبكات العامة المجانية غالباً ما تكون غير مشفرة.
سرقة الأجهزة الذكية | Smart Devices Theft
سرقة الأجهزة غير المحمية بكلمة سر يجعل بيانات و حسابات الضحية معرضة للسرقة أو النشر, تشفير الجهاز بالكامل يُصعب على السارق استرجاع البيانات الخاصة.
****
كلمات المرور الضعيفة | Weak Passwords
يستطيع المخترق أن يتنبأ بكلمات المرور الضعيفة كأسماء الأقارب أو تاريخ الميلاد أو غيرها باستخدام برامج خاصة مما يسهل عملية سرقة الحسابات.
الثغرات الأمنية | Vulnerabilities
الثغرة الأمنية هي أي نقطة ضعف في إعدادات أو مميزات أي نظام. أيضاً أي خطأ برمجي في أي برنامج أو نظام تشغيل.
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
©HemayaGroup
www.hemayagroup.org
حماية Hemaya
تصميم : أبرار الرفاعي
المصدر
مقال بعنوان: الأجهزة الذكية .. المخاطر و الحماية
الكاتب: سامي الأيداء

نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية

المادة الثالثة

الجرائم الموجبة للعقوبة

المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو مافي حكمها

الدخول غير المشروع إلى موقع الكتروني أو الدخول الى موقع الكتروني لتغير تصاميم هذا الموقع او اتلافه اوتعديله او شغل عنوانهَ

الدخول غير المشروع لتهديد أو ابتزاز شخص لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً

التشهير بالاخرين و الحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة

التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أوأحد اجهزة الحاسب الالي (دون مسوغ نظامي صحيح) أو التقاطه أو اعتراضه

العقوبات

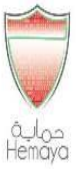
غرامة لاتزيد على 500 ألف ريال

أو

السجن لمدة لاتزيد على سنة واحدة

أو

كلتا العقوبتين السابقتين معاً



المجموعة السعودية لأمن المعلومات

Saudi Group for Information Assurance

HemayaGroup

hemayagroup.org

تصميم:أبرار الرفاعي

@AbrarSR

وعيك سبيل أمنك

السب و الشتم
عبر وسائل تقنية المعلومات

السب والشتم

توجيه كلمات أو عبارات لشخص تمس شرفه أو اعتباره، أو وصفه بصفة تحط من قدره، أو تؤثر في سمعته، عبر الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

العقوبة

السجن لمدة لا تزيد عن خمس سنوات
أو غرامة لا تزيد على ثلاثة ملايين ريال
أو كلتا العقوبتين السابقتين معاً.

للمحكمة المختصة أن تعفي من العقوبة كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر.

يعاقب كل من شرع في القيام بالجريمة

يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب هذه الجريمة.

تصادر الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب الجريمة، أو الأموال المحصلة منها.

صور الجريمة

الإنتاج
بقيام الجاني باستخدام الشبكة المعلوماتية أو إحدى وسائل التقنية بإنتاج مادة سلبية مسيئة للغير.

الإعداد
الإعداد هنا عام يشمل جميع الطرق التي يتخذها الجاني لارتكاب فعله المحظور.

الإرسال
بقيام الجاني بث ما قام بإنتاجه أو إعداده مما يمس الغير قاصداً الإضرار به بجرح مشاعره والنيل من سمعته.

التخزين
بقيام الجاني بالاحتفاظ بما يسيئ للغير من خلال الشبكة المعلوماتية أو إحدى وسائل التقنية.

لردع المعتدي قم بتقديم شكوى لدى إحدى الجهات المختصة

وزارة الداخلية
مركز الشرطة
تطبيق كلنا أمن للهواتف الذكية
بوابة أبشر www.moi.gov.sa

هيئة الأمر بالمعروف والنهي عن المنكر
الاتصال بالرقم الموحد 1909
الموقع الرسمي www.pv.gov.sa

وزارة الثقافة و الإعلام
الموقع الرسمي www.info.gov.sa

الهيئة العامة للإعلام المرئي و المسموع
حساب الهيئة في تويتر @gcamsa
البريد الالكتروني info@gcam.gov.sa
الموقع الرسمي www.gcam.gov.sa

عند تقديم الشكوى يُفضل إيضاح المعلومات التالية

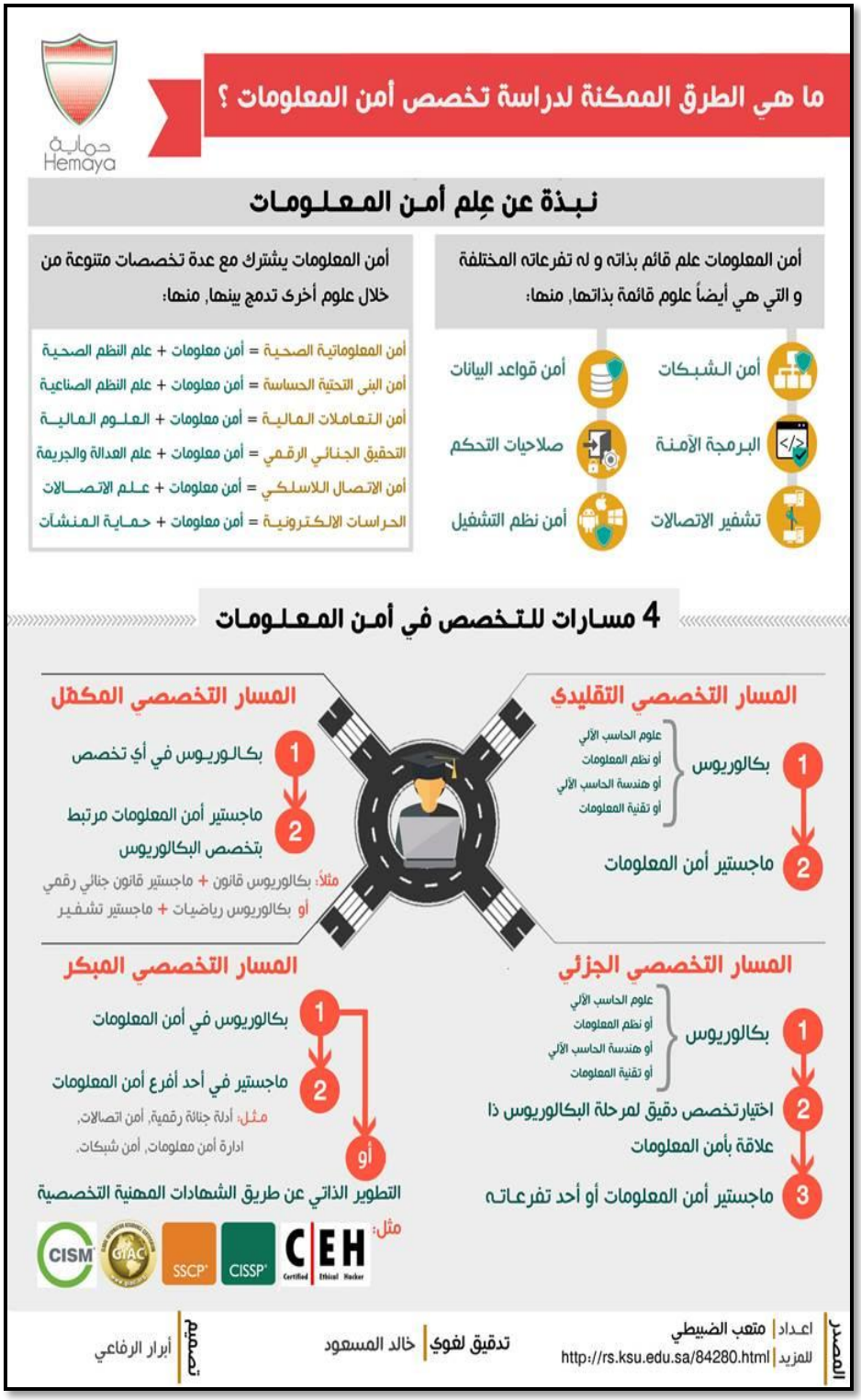
- وقائع الجريمة
- الجاني
- أداة و وسيلة الجريمة
- وقت ارتكاب الجريمة
- مكان ارتكاب الجريمة

المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
www.hemayagroup.org
@HemayaGroup
إعداد
فريق التوعية بالجرائم المعلوماتية
تصميم | أبرار الرفاعي


وعيك سبيل أمنك
الابتزاز
تعريف الابتزاز
هو محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه أو التهديد.
أُشير للابتزاز في المادة الثالثة من نظام الجرائم المعلوماتية :
"الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً".
عقوبة المبتز
السجن لمدة لا تزيد عن سنة واحدة و غرامة لاتزيد على 500 ألف ريال أو احدى هاتين العقوبتين
إذا بادر الجاني بإبلاغ السلطة المختصة قبل العلم بجريمة الابتزاز أو وقوع الضرر قد يعفي من العقوبة
الشروع في الابتزاز معاقب عليه
شريك الجاني والمحرض والمساعد سواء في العقوبة
مصادرة الإجهزة أو الأموال المحصلة من الجريمة.
من أنواع الابتزاز
عاطفي
مادي
أخلاقي
من وسائل الابتزاز
الصور
التسجيل الصوتي
مقاطع الفيديو
لردع المبتز قم بتقديم شكوى لدى إحدى الجهات المختصة
وزارة الداخلية
مركز الشرطة
تطبيق كلنا أمن للهواتف الذكية
بوابة أبشر www.moi.gov.sa
هيئة الأمر بالمعروف والنهي عن المنكر
الاتصال بالرقم الموحد 1909
الموقع الرسمي
www.pv.gov.sa
عند تقديم الشكوى يُفضل إيضاح المعلومات التالية
وقائع جريمة الابتزاز
الجاني
أداة و وسيلة الابتزاز
وقت ارتكاب الجريمة
مكان ارتكاب الجريمة
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
www.hemayagroup.org
@HemayaGroup
إعداد
فريق التوعية بالجرائم المعلوماتية
تصميم | أبرار الرفاعي


تشفير تطبيق الواتساب
(بروتوكول Signal)
مرحلة التسجيل
١ عند تركيب التطبيق يقوم البرنامج لدى المستخدم بإنشاء مفاتيح جديدة
٢ يرسل البرنامج مفاتيح المستخدم العامة لخادم الواتساب
المفاتيح الخاصة
المفاتيح العامة
المفاتيح العامة
خادم الواتساب
الانترنت
قناة الاتصال مع الخادم مشفرة.
(في أجهزة الاندرويد والايفون والويندوز فون فقط)
يتم تجديد المفاتيح من فترة لأخرى ماعدا مفتاح التعريف الذي يبقى كما هو إلى أن يتغير رقم المستخدم أو يعيد تركيب تطبيق الواتساب.
مرحلة إعداد الجلسة عند التخاطب مع أحد المستخدمين للمرة الأولى
يطلب المرسل مفاتيح المستقبل العامة والمحفوظة في الخادم
يرسل الخادم المفاتيح للمرسل
يقوم المرسل بإنشاء مفتاح سري ناتج من مفتاحه الخاص مع مفتاح المستقبل العام.
يشفر المرسل الرسالة بالمفتاح السري ويرفق معها مفاتيحه العامة.
يمرر الخادم الرسالة المشفرة ولا يستطيع قراءة محتواها.
يقوم المستقبل بإنشاء المفتاح السري وذلك باستخدام مفتاحه الخاص مع المفتاح العام المرفق مع الرسالة.
يتم استخدام المفتاح السري لفك تشفير الرسالة.
يتم بعد ذلك استخدام المفتاح السري فقط من الطرفين لتشفير جميع المراسلات إلى أن يتغير مفتاح التعريف لأحد الطرفين، فعند حدوث ذلك تعاد عملية إعداد الجلسة.
ملفات الوسائط (الفيديو والصور والصوت) والمستندات يتم تشفيرها بنفس الأسلوب.
تشفير رسائل المجموعات
تشفير رسائل المجموعات يتبع أسلوب مشابه تقريباً لطريقة المراسلات بين طرفين
١ يقوم المرسل عند إرسال رسالته الأولى بإنشاء جلسة للمجموعة وذلك بالتخاطب مع جميع أعضاء المجموعة كل على حدة وبتشفير مختلف عن الآخرين.
٢ يقوم المرسل بإرسال مفتاح موحد خاص به يسمى "مفتاح المرسل" لجميع الأعضاء.
٣ يلتقي المرسل مفاتيح التشفير لكل رسالة (مفتاح تسلسلي ومفتاح الرسالة) باستخدام مفتاح المرسل نفسه ويستخدم تلك المفاتيح لتشفير رسالته.
٤ تمرر الرسالة للخادم والذي بدوره يقوم بتوزيع تلك الرسالة لجميع أعضاء المجموعة.
٥ جميع الأعضاء يقومون باستخدام مفتاح المرسل لاستخراج المفاتيح التي تتيح لهم فك تشفير تلك الرسالة والرسائل القادمة.
عندما يقوم أحدهم بمغادرة المجموعة يقوم بقية الأعضاء بمسح جميع مفاتيح المرسلين وإعادة إنشاء جلسات المجموعة من جديد.
٣ أسباب تجعل تطبيق الواتساب وتشفيره صعب الوثوق به
بروتوكول Signal مصمم في الأصل ليوفر خاصية الإنكار (Repudiation) والتي تمكن المرسل من إنكار علاقته بالرسائل التي قام هو بإرسالها فإن عملية التحقق تعتمد على الثقة بخادم الواتساب بالإضافة لعملية مطابقة رمز التحقق يدويا من كلا الطرفين.
التطبيق مغلق المصدر مما يصعب عملية التحقق من طريقة عمله ومطابقتها مع ما أعلن عن طريقة عمل بروتوكول التشفير.
التطبيق لا يزال يدعم التراسل غير المشفر للتوافق مع الإصدارات القديمة ولأن عملية الانتقال للتشفير تمت بشكل تلقائي من الشركة بدون موافقة المستخدم فهذا يعني أن الشركة قادرة على تعطيل التشفير لشخص معين دون علمه.
إعداد | فهد الدريبي
تدقيق لغوي | محمد الشهري
تصميم | أبرار الرفاعي
المجموعة السعودية لأمن المعلومات
HemayaGroup
www.hemayagroup.org


طُرق حماية
الأجهزة الذكية
حماية
Hemaya
www.hemayagroup.org
فقط استخدم البرامج المتوفرة في المتاجر الرسمية مثل Google Play و Apple Store .
تجنب تفعيل الروت (Root) أو الجيلبريك (Jailbreak) في جهازك.
تأكد من صحة الرابط قبل الضغط عليه بقراءة اسم الموقع و التأكد من صحته.
http://www.abc...
في حال إرسال البيانات السرية تأكد من علامة القفل الأخضر في الرابط.
https://
احرص على تحديث نظام التشغيل و البرامج المثبتة في جهازك بشكل مستمر من أجل إصلاح جميع الثغرات التي قد تؤدي لاختراق جهازك.
تجنب استخدام الشبكات اللاسلكية المجهولة والمفتوحة في المرافق العامة. قد تتعرض الشبكة لاختراق من مخترقين بهدف جمع المعلومات الخاصة و التجسس على المستخدمين.
FREE
احرص على تنصيب برامج مكافح الفيروسات في جهازك فهي تساعد كثيراً في حمايتك من البرامج الخبيثة.
تجاهل أية رسائل مجهولة المصدر, فهي غالبا ما تحتوي على روابط لبرامج خبيثة أو صفحات مزورة لمواقع.
تأكد من قراءة الصلاحيات التي يطلبها البرنامج قبل البدء بتنصيبه, قد يكون فيها طلب وصول لبياناتك الشخصية و السرية.
احرص على تعطيل خاصيتي الوايرليس والبلوتوث في جهازك في حال عدم استخدامها فقد يلجأ المخترق لاستغلال أي ضعف في هذه التقنيات للاختراق.
في مواقع التواصل الاجتماعي احرص على عدم الكشف عن أي بيانات شخصية واحرص على تعطيل خاصية تحديد الموقع وذلك حفاظاً على خصوصية المستخدمين.
احرص على تفعيل خاصية التحقق الثنائي في جميع حساباتك بشكل عام فهي تساهم كثيرا في حفظ حساباتك من الاختراقات.
المصدر
مقال بعنوان: الأجهزة الذكية .. المخاطر و الحماية
الكاتب | سامي الأيداء
تدقيق | اسامة الرويلي + عبدالله العياضي
تصميم | أبرار الرفاعي


ما هي الطرق الممكنة لدراسة تخصص أمن المعلومات ؟
نبذة عن عِلم أمن المعلومات
أمن المعلومات علم قائم بذاته و له تفرعاته المختلفة و التي هي أيضاً علوم قائمة بذاتها, منها:
أمن الشبكات
أمن قواعد البيانات
البرمجة الآمنة
صلاحيات التحكم
تشفير الإتصالات
أمن نظم التشغيل
أمن المعلومات يشترك مع عدة تخصصات متنوعة من خلال علوم أخرى تدمج بينها, منها:
أمن المعلوماتية الصحية = أمن معلومات + علم النظم الصحية
أمن البنى التحتية الحساسة = أمن معلومات + علم النظم الصناعية
أمن التعاملات المالية = أمن معلومات + العلوم المالية
التحقيق الجنائي الرقمي = أمن معلومات + علم العدالة والجريمة
أمن الإتصال اللاسلكي = أمن معلومات + علم الإتصالات
الحراسات الإلكترونية = أمن معلومات + حماية المنشآت
4 مسارات للتخصص في أمن المعلومات
المسار التخصصي التقليدي
1 بكالوريوس
علوم الحاسب الآلي
أو نظم المعلومات
أو هندسة الحاسب الآلي
أو تقنية المعلومات
2 ماجستير أمن المعلومات
المسار التخصصي المكثف
1 بكالوريوس في أي تخصص
2 ماجستير أمن المعلومات مرتبط بتخصص البكالوريوس
مثلاً: بكالوريوس قانون + ماجستير قانون جنائي رقمي
أو بكالوريوس رياضيات + ماجستير تشفير
المسار التخصصي الجزئي
1 بكالوريوس
علوم الحاسب الآلي
أو نظم المعلومات
أو هندسة الحاسب الآلي
أو تقنية المعلومات
2 اختيار تخصص دقيق لمرحلة البكالوريوس ذا علاقة بأمن المعلومات
3 ماجستير أمن المعلومات أو أحد تفرعاته
المسار التخصصي المبكر
1 بكالوريوس في أمن المعلومات
2 ماجستير في أحد أفرع أمن المعلومات
مثل: أدلة جنائية رقمية, أمن اتصالات, ادارة أمن معلومات, أمن شبكات.
أو
التطوير الذاتي عن طريق الشهادات المهنية التخصصية
مثل:
CISM
GIAC
SSCP
CISSP
CEH Certified Ethical Hacker
المصدر
اعداد | متعب الضبيطي
للمزيد | http://rs.ksu.edu.sa/84280.html
تدقيق لغوي | خالد المسعود
تصميم | أبرار الرفاعي


وعيك سبيل أمنك
حماية الشبكة اللاسلكية
عندما يكون الاتصال الشبكي اللاسلكي لديك غير آمن فمن السهل أن يلتقط المخترق المعلومات الخاصة بشبكتك المنزلية ومن ثم الوصول إلى البيانات التي ترسلها أوتستقبلها بحيث يكون بإمكانه الوصول إلى الملفات المحفوظة في حاسوبك
كيف أحمي الاتصال الشبكي اللاسلكي الخاص بي؟
تعطيل بث معرف الخدمة(Service Set Identifier) لتمنع جهاز الاتصال الشبكي اللاسلكي من التعريف بوجوده
OFF
استخدام أدوات مراقبة الشبكات مثل Fing
تعطيل خاصية الدخول عن بعد
التأكد من اختيار كلمة مرور قوية لشبكتك الخاصة
تغيير اسم الشبكة و كلمة المرور الافتراضية الخاصة بموجه الشبكة اللاسلكية
تفعيل خاصية التشفيرWPA2 لتقوية أمن الشبكة
التأكد من أن المتصلين بشبكتك هم أشخاص تثق بهم ولهم صلاحية الوصول لشبكتك
تغيير كلمة مرور مسؤول الشبكة الخاص بموّجه الشبكة اللاسلكية
أهم أنواع التشفير للشبكات اللاسلكية
1)Wired Equivalent Privacy (WEP)
الـ WEP يقوم بعملية تعرف باسم "shared secret keys"
أو بالترجمة الحرفية «تقاسم المفاتيح السرية»عن طريق التشفير بـ RC4
والتحقق من مصداقية القيم أو باسمها الصحيح
ويعتبر من أقدم و أخطر أنظمة التشفير، حيث تم اختراقه و كسره في عام 2001ولكن من المؤسف أن أغلب مستخدمي الانترنت المنزلي يستخدمون هذا النوع
2) Wi-Fi Protected Access (WPA)
يعد هذا النظام أقوى من الـ WEB
ويدعم نظام المفتاح المشترك Pre-Shared Key WPA-PSK، حيث إنه يستخدم 256bit كطول لمفتاح التشفير مما يصعب كسره،وهذا النوع يعتبر أكثر أمانا من الـWEB
3)Wi-Fi Protected Access II (WPA2)
هو تطوير للبروتوكول السابق و أطلق هذا عمل بخوارزمياتAES التشفير في 2006 حيث
التشفير الأقوى على الإطلاق
ويعتبر هو الأكثر أمانا للاستخدام المنزلي
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
إعـداد
م.راند العتيبي @rf_1123
تصميم: سماهر العراقي
تـدقـيـق لغوي
نورة الطليان
اسامه الرويلي
www.hemayagroup.org
@HemayaGroup

#وعيك_ سبيل_ أمنك

نصائح عند الشراء من المواقع الالكترونية

١- هل الموقع حقيقي ؟

تأكد من أنك تشتري من الموقع المراد فعلاً، وليس أحد المواقع المزورة، ويمكنك التأكد من صحة الموقع عن طريق البحث في محركات البحث الشهيرة مثل موقع (جوجل)

٢- هل الموقع موثوق ؟

أغلب المواقع التجارية يجب أن تنتهي ب .com
فلو وجد موقع ينتهي ب .ws أو .it مثلاً
فهو موقع مشكوك فيه من حيث التعامل التجاري، ويمكن لبحث في بعض المواقع التي تقوم بتقييم المواقع وسلامتها

فعلى سبيل المثال وليس الحصر:

- https://safeweb.norton.com
- http://www.scamadviser.com/
- https://www.site-analyzer.com/
- http://www.seomastering.com/
- https://www.virustotal.com

٣- هل الموقع مشفر ؟

الأمان في نقل البيانات
خاصة عند إدخال بيانات مهمة وحساسة مثل البيانات البنكية، وذلك بالتأكد من ابتداء الرابط بـ https ووجود القفل الأخضر بجوار الرابط

٤- هل وسيلة الدفع امنة ؟

يفضل بشدة استخدام بطاقات ائتمانية مسبقة الدفع، بحيث تقوم بشحنها بالمبلغ المراد الشراء به فقط

٥- هل وسيلة الاتصال امنة ؟

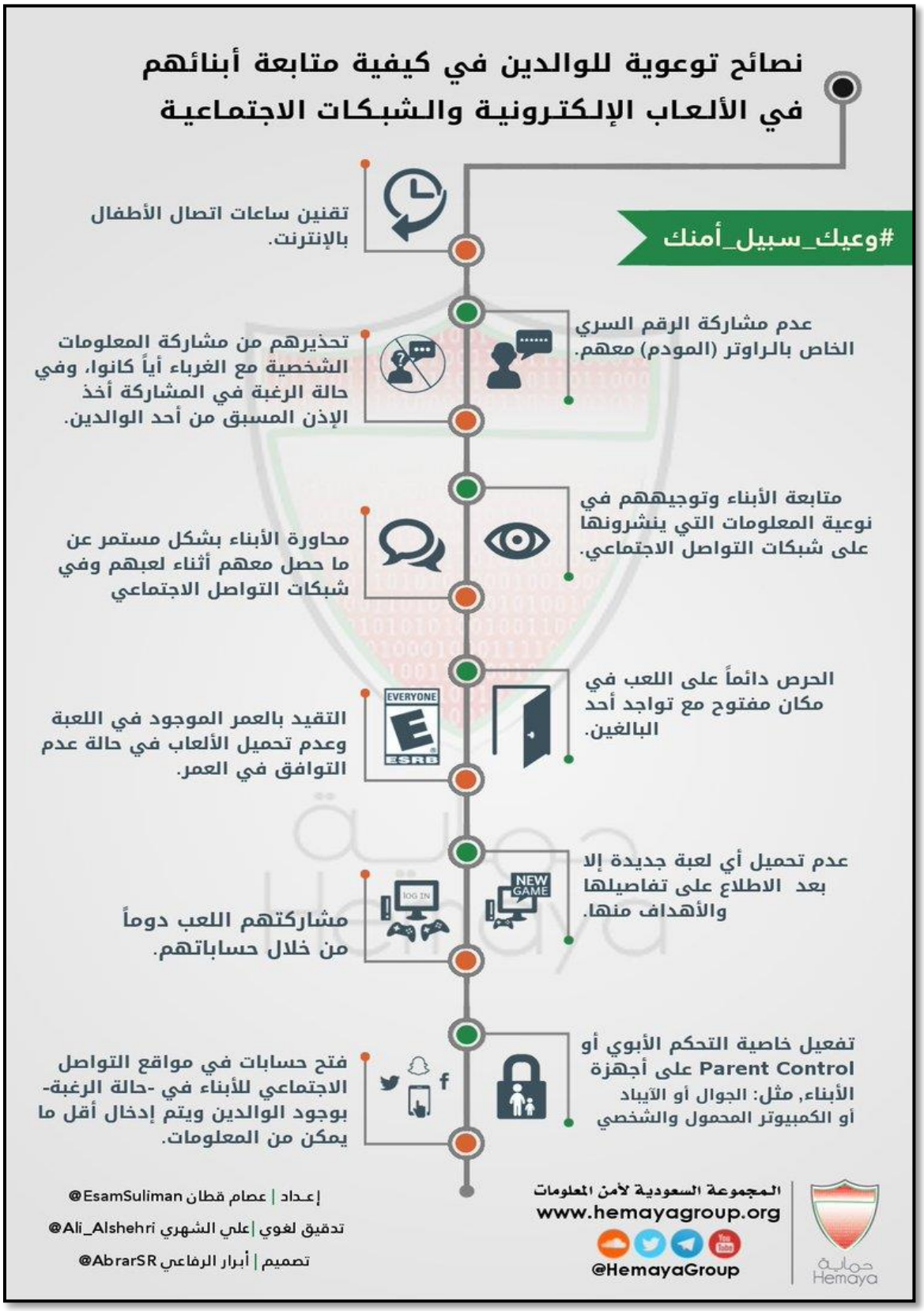
تجنب استخدام الشبكات العامة عند إجراء تعاملات تجارية عبر الإنترنت، مثل المقاهي والمطارات والفنادق، واستخدم الشبكات المؤمنة، مثل شبكات المنزل مع تأمينها، أو شبكات الاتصال عن طريق الجوال وغيره

إعداد: علي الشهري @ali_alshehri
&
متعب الضبيطي @iMoteeb
تدقيق: نهى الغامدي @14nuha14
تصميم: ريهام بارجاء @RABarajaa

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup


كيف تحفظ ١٠٠٠٠٠٠ كلمة مرور بسهولة !
أجعل لنفسك قاعدة ترجع إليها عند اختيار كلمات المرور الخاصة بحساباتك الإلكترونية
مثلاً, سنستخدم القانون التالي كقاعدة عامة لإنشاء كلمة مرور طولها ١٠ أحرف
١ الحرف الاول والثاني من اسم المستخدم ahmad
٢ علامة "&" (مكررة مرتان)
٣ الحرف الاول والثاني من اسم الموقع (أحرف صغيرة)
٤ عدد أحرف اسم الموقع (مكررة مرتان)
٥ الحرف الاول والثاني من اسم الموقع (أحرف كبيرة)
ah&&tw77TW
إذاً, كلمة المرور في تويتر twitter.com
ah&&mo33MO
و كلمة المرور في أبشر moi.gov.sa كالتالي
يمكنك ابتكار قاعدة خاصة بك بطرق مختلفة وسهلة الحفظ وملائمة, مثلاً: أول حرف وأخر حرف, ثم أول حرف مكرر, ثم علامتان #^, ثم نوع النطاق com أو net, ... إلخ
بعض المواقع مثل البنوك تمنع استخدام بعض الرموز مثل $ و الأقواس فيُنصح إنشاء قاعدة ملائمة.
فائدة هذه الطريقة
سهلة التذكر
لن تحتاج إلى تكرار نفس كلمة المرور لكل حساب ولا لكتابتها.
يصعب استنتاج القاعدة الأساسية
حتى لو تم كشف كلمة المرور باختراق الحساب فإنه يصعب استنتاج هذه القاعدة.
صعبة التخمين
لن يكون بمقدور المخترق تخمينها ولا تستطيع أدوات كشف كلمات المرور تخمينها.
حماية Hemaya
إعداد
متعب الضبيطي @iMoteeb
للمزيد: http://goo.gl/QZxBNU
تدقيق لغوي | علي الشهري @Ali_Alshehri
تصميم | أبرار الرفاعي @AbrarSR
www.hemayagroup.org
@HemayaGroup


الهندسة الاجتماعية
هي استخدام وسائل خداعية تتضمن الإقناع وانتحال الشخصيات التي يغلب على الظن أن تتعامل معها الضحية أو تصدقها بهدف سرقة المعلومات والاستفادة منها في ابتزاز نفس الضحية أو ضحية أخرى.
تعرف الهندسة الاجتماعية بـ(اختراق العقول) لأن علامة نجاحه هو اقتناع عقل الضحية بما يدعيه المهاجم
الدوافع
شخصية
تجارية
سياسية
الهندسة الاجتماعية من أخطر أنواع الهجمات، لأن خداع البشر أو اختراقهم أسهل من اختراق الأنظمة ولا يحتاج إلى الخبرة والأدوات والتكاليف التي تستخدم في اختراق الأنظمة. الهندسة الاجتماعية لا تعتمد على وسائل الاختراق أو التقنيات المتطورة، فهي تعتمد على الكثير من الكذب والخداع، لا سيما أن استخدام التقنية مع الهندسة الاجتماعية يجعلها أكثر خطورة.
أنواع الهندسة الاجتماعية
الهندسة الاجتماعية البشرية
استخدام الأساليب و المهارات البشرية دون الاعتماد على التقنية، وهذا لا يعني عدم استخدام أي وسيلة تقنية في هذا النوع بل المقصود أن وسيلة الهجوم الأساسية والتي يتم المهاجمة بها تكون مهارة بشرية.
الأساليب
البحث في سلة المهملات عن أوراق أو معلومات مفيدة
التحدث من خلال الهاتف
مقابلة شخص مقرب للضحية يملك المعلومات المطلوبة
مراسلة الضحية عبر أحد البرامج
مراقبة الضحية و سلوكه
التحدث بشكل مباشر مع الضحية
الهندسة الاجتماعية التقنية
استخدام وسائل خداعية تعتمد على التقنية بشكل مباشر. أي أن المهاجم يستخدم أدوات تقنية معدة ومبرمجة مسبقا تمكنه من سحب معلومات الضحية.
الأساليب
إرسال الرسائل الاصطيادية
إعلانات وهمية
تزييف الصفحات الرسمية
النوافذ المنبثقة
كيفية كشف تزييف الصفحات الرسمية
لكشف الرابط المزور راجع امتداد العنوان قبل علامة "/" إذا لم يكن نفس عنوان الموقع الرسمي أو متضمنا بعض الزيادات فالرابط يكون مزور.
الموقع مزور
لأن عنوان الموقع متضمن بعض الزيادات
الموقع أصلي
فالعنوان صحيح ولا يتضمن زيادة في حروفه
الموقع مزور
لأن العنوان الظاهر ليس عنوان الموقع الرسمي
كيفية تفادي هذا النوع من الاحتيال
عدم الوثوق أبدا في أي شخصية على فضاء الانترنت.
التعامل دائما بمبدأ الحذر.
التساؤل دائما عن الدوافع والفائدة.
عدم مشاركة كلمة/كلمات السر خاصتك مع الآخرين.
إذا شعرت بهجوم أو أن حسابك قد تم اختراقه عليك تغيير كلمة السر فورا.
يجب النظر بعين الشك إلى كل بريد إلكتروني أو رسالة أو تعليق يصلك يحتوي على ملفات وروابط مرفقة.
عليك التحقق من شخصية من يقوم بمراسلتك سواء عبر البريد الإلكتروني، أو برامج المراسلة، أو عبر وسائل التواصل الاجتماعي.
يجب الحرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك لأن المهاجم قد يستخدمها لانتحال شخصيتك ومهاجمة صديق لك أو قد يستخدم المعلومات ليصيغ الهجوم عليك بشكل مقنع أكثر.
عند الشك برسالة ما أو بجهة اتصال مشبوهة، احذر فتح الملفات أو الروابط المرفقة في الرسالة. وقم بالاتصال بالجهة والتحقق عن طريق القنوات الرسمية.
في حال رغبتك بفتح أي ملف أو رابط يصلك قم قبل ذلك بالتأكد من أنه ليس خبيثا باستخدام مواقع فحص الروابط، مثل موقع https://www.virustotal.com
إذا تم الهجوم وتعرضت إلى أضرار يمكنك التبليغ عن جريمة إلكترونية من خلال بوابة أبشر عبر حسابك الخاص، ثم بالدخول إلى الخدمات الإلكترونية ثم الأمن العام ثم الجرائم الإلكترونية.
إعداد
يزيد التميمي @yazeedst
تدقيق لغوي | علي الشهري @Ali_Alshehri
تصميم | أبرار الرماعي @AbrarSR
www.hemayagroup.org
@HemayaGroup


نصائح توعوية للوالدين في كيفية متابعة أبنائهم
في الألعاب الإلكترونية والشبكات الاجتماعية
#وعيك_سبيل_أمنك
تقنين ساعات اتصال الأطفال بالإنترنت.
عدم مشاركة الرقم السري الخاص بالراوتر (المودم) معهم.
تحذيرهم من مشاركة المعلومات الشخصية مع الغرباء أياً كانوا، وفي حالة الرغبة في المشاركة أخذ الإذن المسبق من أحد الوالدين.
متابعة الأبناء وتوجيههم في نوعية المعلومات التي ينشرونها على شبكات التواصل الاجتماعي.
محاورة الأبناء بشكل مستمر عن ما حصل معهم أثناء لعبهم وفي شبكات التواصل الاجتماعي
الحرص دائماً على اللعب في مكان مفتوح مع تواجد أحد البالغين.
EVERYONE
ESRB
التقيد بالعمر الموجود في اللعبة وعدم تحميل الألعاب في حالة عدم التوافق في العمر.
عدم تحميل أي لعبة جديدة إلا بعد الاطلاع على تفاصيلها والأهداف منها.
NEW GAME
LOG IN
مشاركتهم اللعب دوماً من خلال حساباتهم.
تفعيل خاصية التحكم الأبوي أو Parent Control على أجهزة الأبناء, مثل: الجوال أو الآيباد أو الكمبيوتر المحمول والشخصي
فتح حسابات في مواقع التواصل الاجتماعي للأبناء في -حالة الرغبة- بوجود الوالدين ويتم إدخال أقل ما يمكن من المعلومات.
إعداد | عصام قطان @EsamSuliman
تدقيق لغوي | علي الشهري @Ali_Alshehri
تصميم | أبرار الرفاعي @AbrarSR
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup
حماية Hemaya

وعيك سبيل أمنك

التجسس الإلكتروني

هو الاطلاع من خلال الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي على أسرار الآخرين بدون موافقتهم.

العقوبة

السجن لمدة لا تزيد على سنة
أو غرامة لا تزيد على 500 ألف ريال
أو كلتا العقوبتين السابقتين معاً.

للمحكمة المختصة أن تعفي من العقوبة كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر.

يعاقب كل من شرع في القيام بالجريمة.

تصادر الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب الجريمة، أو الأموال المحصلة منها.

يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب هذه الجريمة.

صور الجريمة

التنصت والالتقاط الالكتروني

مشاهدة البيانات أو الحصول عليها بأي شكل من أشكالها (مسموعة، مقروءة، مرئيّة) دون مسوغ نظامي صحيح.

أنواع التنصت

نشط

وهو ذلك التنصت أو الالتقاط الذي يحدث ضرراً على سرية وسلامة البيانات أو المعلومات من خلال تغييرها أو تشويهها قبل وصولها إلى الطرف المستقبل.

غير نشط

هو ذلك التنصت أو الالتقاط الذي يحدث ضرراً على سرية البيانات أو المعلومات ولكن لا يحدث ضرراً على سلامتها. و تتم الاستفادة من تلك البيانات والمعلومات من أجل الإضرار بالمتنصت عليهم لاحقاً.

الاعتراض

اعتراض ماهو مرسل عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.

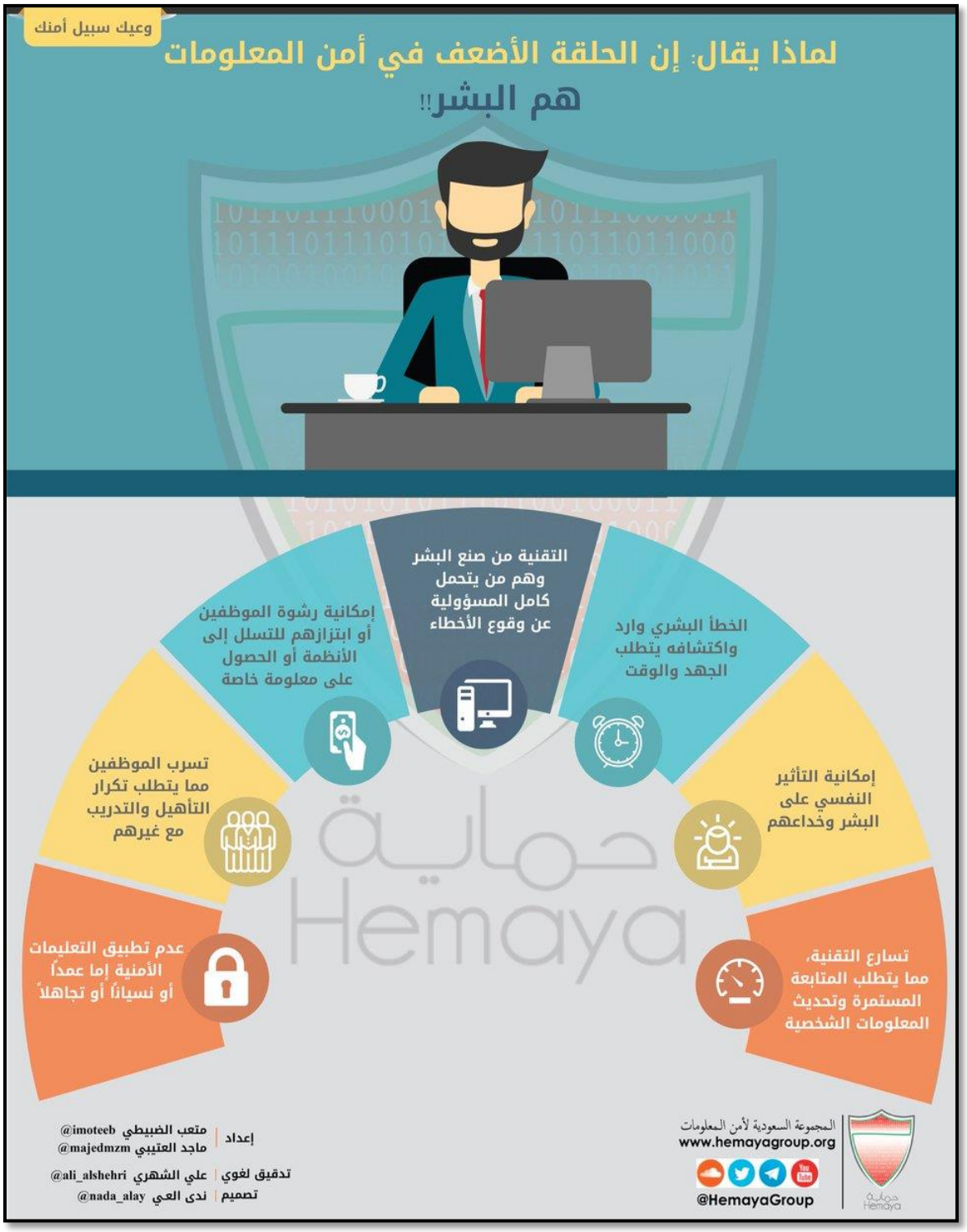
إعداد
فريق التوعية بالجرائم المعلوماتية

تصميم | أبرار الرفاعي

www.hemayagroup.org
@HemayaGroup


استخدام الحوسبة السحابية بأمان
الحوسبة السحابية تعني الاستفادة من مزود خدمة على شبكة الانترنت لتخزين وإدارة البيانات.
مميزات الحوسبة السحابية
التكلفة المنخفضة
سرعة الخدمات
إمكانية مشاركة المعلومات.
مزامنة البيانات والوصول إليها بسهولة من أجهزة متعددة
توسيع نطاق العمل
استخداماتها
خدمات البريد الإلكتروني Email Services
خدمات التخزين السحابي Cloud Storage
التطبيقات السحابية Cloud Applications
أنظمة التشغيل السحابية Cloud Operating Systems
أمثلة الحوسبة السحابية
salesforce
OneDrive
Dropbox
iCloud
amazondrive
vmware
أبرز التهديدات
سرقة البيانات Data Breaches
فيروسات الفدية Ransomware
البرمجيات الخبيثة Malware
هجمات حجب الخدمة Denial of Service
ضياع البيانات Data Loss
تسريب المعلومات Information leakage
الاستخدام بشكل خاطئ Misuse
نقاط ضعف في التقنيات المستخدمة Threats and Vulnerabilities
فيما يلي بعض الخطوات و الإجراءات المستخدمة للوصول إلى الحد الأدنى من أمان الحوسبة السحابية.
المصادقة
اختيار كلمة مرور قوية تتطابق مع معايير كلمات المرور يسهل تذكرها و يصعب تخمينها.
تحتوي على 8 خانات على الأقل مكونة من حروف كبيرة، و حروف صغيرة ، وأرقام ورموز خاصة و علامات الترقيم.
استبدال كلمات المرور بعبارات مرور إن أمكن .
استخدام التحقق الثنائي 2FA .
تجنب استخدم كلمة مرور واحدة لجميع الحسابات .
تغيير كلمات المرور بشكل منتظم مثلا كل 90 يوم.
استخدام كلمات مرور تختلف اختلافا كبيراً عن كلمات المرور المستخدمة في وقت سابق.
تجنب حفظ كلمات المرور كجهة اتصال لتجنب سرقتها عن طريق برامج البحث بالارقام.
تأكد دائماً من إلغاء خاصية الحفظ أو الإكمال التلقائي لكلمات المرور في المتصفحات.
مشاركة الملفات و تبادل البيانات
عدم مشاركة الملفات مع الكل بشكل افتراضي.
السماح للأشخاص المعنيين فقط بالوصول إلى البيانات أو بعضها حسب الحاجة، وإزالة الصلاحيات فور الإنتهاء .
عند المشاركة باستخدام الروابط إحرص على سلامة الرابط .
وضع كلمة مرور لمشاركة الروابط وإزالة الخاصية فور الإنتهاء.
تحديد الصلاحيات بحذر، بحيث لا يمكن لأي شخص الكتابة أو التعديل على بياناتك.
التصفح الآمن و تشفير البيانات
تأكد من أن يكون الاتصال آمناً والموقع صحيح.
تأكد من وجود علامة القفل و البروتوكول المستخدم هو (https://).
تجنب إدارة حساباتك من الشكبات المفتوحة أو مقاهي الإنترنت.
قم بتحديث متصفح الإنترنت بشكل مستمر.
لا توافق على خاصية (تذكرني) و (الدخول التلقائي).
قم بمسح الكوكيز (Cookies) وأي معلومات مؤقتة أخرى بشكل مستمر.
اضبط مستوى الأمان في متصفح الإنترنت على أن لا يقل عن مستوى «متوسط».
النسخ الاحتياطي و برامج مكافحة الفيروسات
استخدام برامج مكافحة الفيروسات و تحديثها دورياً.
أخذ نسخاً احتياطية للمعلومات والملفات بشكل مستمر.
تحديث أنظمة التشغيل والتطبيقات بشكل دوري وفعال.
تذكر!
كن على إطلاع على آخر المستجدات في مجال الإختراقات.
قد يتطلب منك تغيير كلمة المرور فوراً عند الإعلان عن أي تسريب للبيانات.
راجع شروط استخدام الخدمة و الصلاحيات الممكنة و الحقوق القانونية.
المجموعة السعودية لأمن المعلومات
www.HemayaGroup.org
@HemayaGroup
إعداد | رائد العتيبي @rf_1123
تدقيق لغوي | نورة الطليان @noorasaadtulaia
تصميم | أبرار الرفاعي @AbrarSR

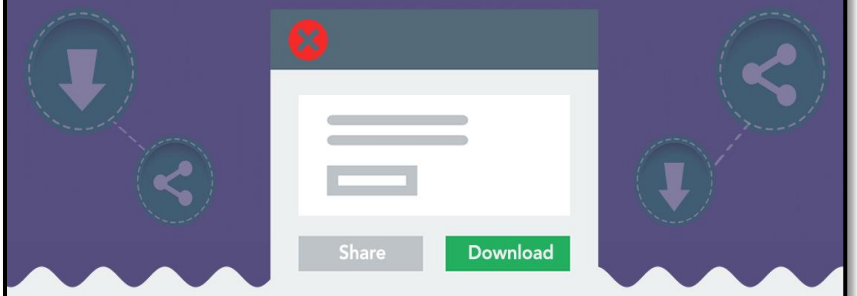

خطوات التعامل مع العصابات الدولية
للابتزاز الالكتروني
#وعيك_سبيل_أمنك
نوع الابتزاز
تشهير
الوسائل المستخدمة
وسائل الاتصال المرئي
هدفه
مالي
طريقة الابتزاز
إغراء جنسي
$$$
خطوات الاستدراج للابتزاز تدريجياً
1 مراسلة الضحية عبر شبكات التواصل الاجتماعي
2 محادثة الضحية وسحب معلومات شخصية وإضافة أصدقائه وأقاربه
3 طلب التواصل المرئي عبر إحدى البرامج
4 إغراء الضحية جنسياً ومن ثم تصويره بوضع مخل
5 تصريح المبتز بحقيقته و تهديد الضحية بفضحه
6 إرسال رابط فيديو لمشاهد الضحية منشوره على اليوتيوب
7 طلب مبالغ ماليه مقابل حذف تلك المشاهد
8 البدء بالضغط النفسي على الضحية وذلك بتهديده بنشر مشاهده بين معارفه
خطوات تجاوز الابتزاز تدريجياً
1 لا تستفز المبتز و قم بمداراته أول الأمر
2 امنع وصوله لأكبر قدر من معلوماتك بتجميد كافة حساباتك الالكترونية
3 لا ترتبك فهذه المشاهد لا تلقى رواجاً ولا تنتشر
4 لا تستجب لتحويل الأموال مهما كلف الأمر
5 اقطع التواصل معه نهائياً ولا تقرأ أي رسائل تصلك منه
6 عليك برباطة الجأش والصبر وعدم الارتباك أو الانهزام
7 تابع المواقع التي يهدد بنشر ما لديه من خلالها
8 أبلغ فوراً عن أي منشور كمحتوى جنسي أو محتوى انتهاك خصوصية
النتائج
سيتم الحذف خلال ساعات معدودة ويصعب رفعها مرة أخرى
سيتوقف المبتز عن محاولات الضغط النفسي في حال لم يستطع إيصال تهديداته للضحية
سيخسر كل أوراق الضغط والتهديد المتاحة لديه
ييأس المبتز من الضحية ويقوم بالبحث عن ضحية أخرى
ملاحظات
هناك احتمالية التورط بالتحويل إلى حسابات مشبوهة أو إرهابية أو جريمة منظمة
المرسل لا يرسل رقم حسابه البنكي أو معلوماته ، بل يورطك مع جهات مشبوهة
خطوات تجاوز الابتزاز تستغرق أقل من ٢٤ ساعه
يمكن إعادة تفعيل الحسابات المجمدة مع تغيير أسم المستخدم في كل حساب كي لا يتم التعقب مرة أخرى
$$$
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup
إعداد | متعب الضبيطي @iMoteeb
تدقيق لغوي | نورة الطلبان @noorasaudtulata
تصميم | ريهام بارجاء @Re_A_H ✦ أبرار @AbrarSR


وعيك سبيل أمنك
لماذا يقال: إن الحلقة الأضعف في أمن المعلومات
هم البشر!!
التقنية من صنع البشر وهم من يتحمل كامل المسؤولية عن وقوع الأخطاء
الخطأ البشري وارد واكتشافه يتطلب الجهد والوقت
إمكانية رشوة الموظفين أو ابتزازهم للتسلل إلى الأنظمة أو الحصول على معلومة خاصة
إمكانية التأثير النفسي على البشر وخداعهم
تسرب الموظفين مما يتطلب تكرار التأهيل والتدريب مع غيرهم
تسارع التقنية، مما يتطلب المتابعة المستمرة وتحديث المعلومات الشخصية
عدم تطبيق التعليمات الأمنية إما عمداً أو نسياناً أو تجاهلاً
حماية Hemaya
إعداد | متعب الضبيطي @imoteeb
ماجد العتيبي @majedmzm
تدقيق لغوي | علي الشهري @ali_alshehri
تصميم | ندى العي @nada_alay
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup


ماذا تفعل
لو وجدت محفظة مفقودة ؟!
#وعيك_سبيل_أمنك
إن حب الخير في مساعدة من فقد محفظته قد يؤدي إلى الإضرار به في حال لم يتم التعامل مع الوثائق التي بها باهتمام بالغ و سرية. إن تصوير ونشر هذه الوثائق عبر الإنترنت بغرض المساعدة قد يؤدي إلى استغلالها.
أمثلة لمعلومات مهمة في أي محفظة مفقودة
الهوية الوطنية
سجل الأسرة
بطاقة الصراف الآلي
معلومات بنكية
طرق استغلال هذه المعلومات
انتحال هوية صاحب المحفظة
توريطه في عمليات مالية
توريطه في عمليات تزوير
ماذا يجب عليك فعله في حال عثورك على محفظة ؟
احتفظ بها في مكان آمن لمدة ٢٤ ساعة.
ابحث عن رقم هاتف للتواصل.
إسأل عن صاحب المحفظة بالاسم فقط ولا تكشف عن أي معلومات أخرى.
لا تصور الوثائق الأخرى وتنشرها عبر الإنترنت في حال لم تجد استجابة خلال ٢٤ ساعة.
سلّم الوثائق الحكومية التي لديك للجهات التابعة لها.
سلّم الوثائق البنكية إلى الجهات التابعة لها.
ماذا يجب عليك فعله في حال فقدانك لمحفظتك ؟
1 راجع حساباتك البنكية فوراً للتأكد من عدم استخدامها من شخص آخر.
2 قم بإلغاء البطاقات البنكية واستخراج أخرى جديدة.
3 راجع سجلات البنوك من خلال مؤسسة النقد للنظر في أي عملية أجريت باسمك قريباً.
إعداد | د. جلال العويبدي @alowibdi
تدقيق لغوي | نورة الطليان @noorasaadtulaia
تصميم | أبرار الرفاعي @AbrarSR
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup


الإنترنت بالسفر
10 نصائح أمنية لحماية بياناتك وأجهزتك من مخاطر إستخدام شبكات الانترنت العامة أثناء السفر
1 عدم الاتصال بأي نقطة وصول (شبكة لاسلكية) غير موثوقة، وخصوصا عند محاولة إجراء عمليات بنكية أو اتصال يحوي بيانات هامة.
2 التأكد من موثوقية الشبكة اللاسلكية بواسطة الاستفسار من موفر الشبكة عن مصدرها وموثقيتها.
3 إذا كان هناك أي اتفاقية او تعليمات لاستخدام الشبكة تأكد من قراءتها جيدا وأنها لاتنتهك خصوصيتك بإفشاء معلوماتك.
4 التأكد من التصفح المشفر للمواقع HTTPS، عوضا عن البروتوكول غير الامن HTTP قدر الإمكان.
Wi Fi CERTIFIED
5 تامين الاتصال بالإنترنت بواسطة استخدام شبكة خاصة افتراضية (VPN) عوضا عن الاتصال المباشر بشبكة الإنترنت.
PASSWORD PROTECTED
6 الحذر دائما من اي طلبات غير معتادة، مثل موقع يطلب منك عنوانك البريدي وكلمة المرور، أو أحد حساباتك في مواقع التواصل مع كلمة المرور.
https
7 إلغاء خاصية الاتصال التلقائي بـ الشبكات اللاسلكية (WiFi) من الحاسب المحمول أو الهاتف الذكي لتفادي الاتصال بشبكات مشبوهة.
8 الحذر من ترك حاسبك المحمول أو أي جهاز يخصك من غير مراقبة أو بعيدا عنك.
9 عدم السماح للمتصفح بحفظ كلمة المرور أو اسم المستخدم عند طلبه ذلك.
10 أخيراً تأكد من قطع الأتصال بعد انتهاء الاستخدام لحماية جهازك من أي محاولات اختراق او تحميل للبرامج الضارة على جهازك.
معلومة...!
عند المرور من خلال المنافذ الحدودية في بعض الدول فإن السلطات المعنية لها الحق في تفتيش ومصادرة ونقل البيانات من أي جهاز. وللحفاظ على بياناتك قم بتخزينها على سحابة إلكترونية مشفرة ليسهل الوصول إليها بأي وقت.
إعداد : عبدالله المحمدي @abdulalmo
تدقيق : نهى الغامدي @14nuha14
علي الشهري @ali_alsheri
تصميم : أيمن الفاضل @alfaddhel
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup
حماية Hemaya

مخاطر استخدام مواقع التورنت لتحميل و مشاركة الملفات



توفر مواقع التورنت طريقة سريعة وسهلة و فعالة لتحميل الملفات من الإنترنت خصوصا ذات الحجم الكبير، غير أنه يمكن تعريض نفسك أو مؤسستك للكثير من المخاطر باستخدامك لمثل هذه المواقع.

يمكن تلخيص أهم هذه المخاطر كالآتي:

إمكانية تحميل ملفات خبيثة :

مرفقات الإيميل ليست هي المصدر الوحيد لتحميل مثل هذه الملفات ، فوفقاً لإحصائية نشرتها شركة InfoArmor في أواخر عام 2016 اتضح أن الملفات الخبيثة التي يتم تحميلها من مواقع التورنت هي السبب في تضرر أكثر من 12 مليون مستخدم شهرياً

*المصدر : https://goo.gl/BRTDxB

الدخول غير المصرح به للجهاز، و الذي قد يتم عن طريق:

- تحميلك لبعض الملفات -و التي قد تبدو ظاهرياً سليمة- حيث تستخدم لفتح منفذ للوصول لبيانات الجهاز وسرقة محتوياته أو التحكم به عن بعد
- مجرد إستخدامك للتورنت لمشاركة الملفات، و حتى مع عدم تحميلك لأي ملف يسهل الوصول لبعض المعلومات الخاصة بالجهاز مثل ال(IP-address) وباستخدام مجموعة من هذه العناوين قد يجد المخترق ضالته و قد يكون جهازك - الذي لم تقم بتحديثه مؤخراً مثلا - هو الضحية

المساءلة القانونية

استخدامك لمواقع التورنت لتحميل الأفلام ،الملفات الصوتية أو البرامج محمية الحقوق في بعض الدول هي جريمة معلوماتية يعاقب عليها القانون و يمكن أن تكون لها عواقب وخيمة.

إعداد : ندى الرحيلي @Nada_Alruhaily
تصميم: سماهر العرابي @i_smaher
تدقيق : نورة الطليان @noorasaadtulaia
يزيد التميمي @yazeedst

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup


وعيك سبيل أمنك
إرشادات لإنشاء كلمة مرور قوية
يجب أن تحتوي على حروف كبيرة وصغيرة وأرقام ورموز مثال (&*%$)
عند إنشائها ابتعد عن تسلسل الحروف والأرقام
زيادة عدد خاناتها يزيد من تعقيدها، وبالتالي يصعب الوصول إليها
يجب المحافظة على سريتها وعدم الإفصاح عنها لأي كان ولأي سبب
يجب تغييرها بين الفينة والأخرى
يجب عدم حفظها على جهازك أو في مسودة
اجعلها مختلفة من حساب إلى آخر
وابتعد أيضًا عن تواريخ الميلاد والأسماء الشخصية وأرقام الهواتف
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
حماية Hemaya
hemayagroup.org
HemayaGroup
إعداد سعود الصويمل @en_saud
تدقيق لغوي نورة الطليان
تصميم ندى العي @nada_alay


وعيك سبيل أمنك
احمِ نفسك ضد الرسائل غير موثوقة المصدر
لا تبادر بفتح الرسائل مجهولة المصدر واحذفها مباشرة
فتح الروابط مجهولة المصدر قد يؤدي إلى اختراق جهازك وسرقة بياناتك
تأكد من إعدادات المتصفح وإغلاق النوافذ المنبثقة
إيقاف خاصية التحميل التلقائي للملفات أو الصور أو مقاطع الفيديو يحميك من الفيروسات
بريدك الإلكتروني خاص بك فلا تنشره في المواقع الأخرى حتى لا تصلك رسائل غير مرغوب بها
SPAM
احذر الرسائل التي تطلب منك معلوماتك الشخصية
تفعيل خاصية تصفية الرسائل تحميك من الرسائل غير المرغوب بها
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
حماية Hemaya
hemayagroup.org
HemayaGroup
إعداد سعود الصويمل @en_saud
تدقيق لغوي نورة الطليان
نهى الغامدي
تصميم ندى العي @nada_alay


وعيك سبيل أمنك
لتصفح آمن
عند رغبتك بتصفح مواقع غير موثوقة قم بتعطيل الخصائص التالية: JavaScript, ActiveX
قم بتحديث متصفح الإنترنت ونظام التشغيل بشكل مستمر
تجنب إدخال بياناتك الخاصة في مواقع أو نماذج غير موثوقة و غير معروفة
قم بمسح الكوكيز (Cookies) وأي معلومات مؤقتة أخرى بشكل مستمر خاصة بعد زيارة المواقع المهمة
لا توافق على خاصية تذكرني و الدخول التلقائي
اضبط مستوى الأمان في متصفح الانترنت على أن لا تقل عن مستوى متوسط
لا تقم بإدخال بياناتك السرية عند زيارتك مواقع لا تستخدم التشفير https://
عطل خاصية إظهار النوافذ المنبثقة (pop up)
بشكل عام لا تستخدم الأجهزة أو الشبكات العامة لتصفح الانترنت
HTTP
WiFi
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
www.hemayagroup.org
@HemayaGroup
إعداد: سامي الأيداء
تصميم: سماهر العرابي

وعيك سبيل أمنك

فيروس طلب الفدية (Ransomeware)

هو عبارة عن برمجية خبيثة تعمل على تشفير ملفاتك المهمة و منع الوصول لها، وتطلب من المستخدم فدية مالية مقابل فك هذا التشفير

نصائح

١ 

احرص على عمل نسخة احتياطية لجميع ملفاتك المهمة على وحدة تخزين خارجية

٢ 

استخدم برنامج لمكافحة الفيروسات و احرص على تحديثه بشكل دوري

٣ 

احرص على تحديث نظام التشغيل و متصفح الإنترنت بشكل دوري

٤ 

عندما تلاحظ أن جهازك يقوم بتصرفات غريبة كزيارة مواقع غريبة أو مشبوهة، اقطع اتصال الإنترنت و اعمل على فحص الجهاز للتأكد من خلوه من البرمجيات الخبيثة

٥ 

تجنب فتح الروابط أو تنزيل المرفقات المرسلة من بريد الكتروني مجهول المصدر

٦ 

تجنب استخدام البرامج غير الأصلية وغير المعروفة فعادة ما تنتقل الفيروسات من خلال هذه البرامج

٧ 

تجنب النقر على أي رابط غير موثوق المصدر، و تجنب زيارة المواقع المشبوهة

٨ 

عند استلامك لبريد الكتروني غير متوقع من مصدر معروف تواصل مع المرسل للتأكد من صحته

إعداد: سامي الأيداء
@sami_alayda
تصميم: ريهام بارجاء
@RABarajaa

WWW.hemayagroup.org
@HemayaGroup
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance

وعيك سبيل أمنك

نصائح أمنية لإدارة حسابات الشبكات الاجتماعية للجهات الرسمية (٢\١١)

كلمة المرور

- اتبع نصائح إنشاء كلمة مرور قوية، وتأكد بأنك لم تستخدمها من قبل
- فعل خاصية التحقق الثنائي للدخول على الحساب
- قم بتغيير كلمة المرور بشكل دوري
- قم بتغيير كلمة المرور عند ملاحظة أمور غريبة في الحساب

الأجهزة المرتبطة بالحساب

- عند تغيير كلمة المرور، احذف الأجهزة التي لها صلاحية على الحساب
- بعد تغيير كلمة المرور، اضبط إعدادات الصلاحية عند الدخول على الحساب

البريد الإلكتروني المرتبط بالحساب

طبق النصائح الأمنية الخاصة بكلمة المرور على البريد الإلكتروني

- تأكد من أمان البريد الإلكتروني المرتبط بالحساب
- استخدم بريد إلكتروني خاص لإدارة حسابات الشبكات الاجتماعية فقط

الصلاحيات للتطبيقات الأخرى

في حالة منح صلاحية، قم بمتابعة هذه الصلاحية باستمرار

- تجنب منح صلاحيات لتطبيقات أخرى قدر المستطاع
- قم بتطبيق هذه النصائح الأمنية على تلك التطبيقات

إعداد: عصام قطان
@EsamSuliman
تصميم: ندى العي
@Nada_Alay

www.hemayagroup.org
HemayaGroup

المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
حماية Hemaya

وعيك سبيل أمنك

نصائح أمنية لإدارة حسابات الشبكات الاجتماعية للجهات الرسمية (٢\٢)

أجهزة الحاسب المستخدمة لإدارة الحساب

- تأكد من وجود برنامج مكافحة الفيروسات على الجهاز يتحدث تلقائيًا
- تأكد من تحديث نظام التشغيل على الجهاز تلقائيًا
- استخدم جهاز العمل للدخول على الحساب فقط
- قم بتحديث متصفح الإنترنت باستمرار

عنوان رابط الدخول على الحساب

تأكد من وجود علامة القفل وأن الموقع يستخدم خاصية (https)

- تأكد دائمًا من صحة الرابط المستخدم للدخول إلى الحساب
- افحص الروابط ببرامج مكافحة الفيروسات للتأكد من أمانها

بريد إلكتروني لطلب كلمة المرور

- تجنب الرسائل التي تطلب تغيير كلمة المرور عن طريق رابط إلا في حال طلبك
- تجنب الرسائل المشبوهة التي تطلب تحميل برامج معينة
- تجنب الرسائل المشبوهة التي تطلب اسم المستخدم وكلمة المرور
- تجنب الرسائل التي تطلب الدخول على مواقع مشبوهة

الروابط المرسلة مع التغريدات

- احذر الروابط المختصرة لأنه يصعب تمييز الآمن منها
- افحص الروابط المختصرة بهذا الموقع http://www.checkshorturl.com
- كن حريصًا عند النقر على الروابط الموجودة في التغريدات
- استخدم المتصفحات المزودة بخاصية التحقق من الروابط المختصرة

المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
www.hemayagroup.org
HemayaGroup
إعداد: عصام قطان
@EsamSuliman
تصميم: ندى العي
@Nada_Alay

مصطلحات في الحماية الإلكترونية

حماية Hemaya

الأمن الإلكتروني: Cyber Security

هو مجموعة من التقنيات والعمليات والممارسات المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به

الغموض: Obscurity

هي سياسة عدم الإفصاح عن أنواع الأجهزة العتاد أنظمة التشغيل والبرمجيات المستخدمة في بيئة تقنية المعلومات الخاصة بمنظمة ما

التأمين الطبقي: Defense in Depth

هي إحدى الاستراتيجيات التي تستخدم في أمن المعلومات وهي عبارة عن إيجاد أكثر من نقطة تأمين تعمل كخطوط دفاع مرحلية بشكل طبقي

أحضر جهازك الخاص: BYOD

سياسة أو استراتيجية تنتهجها بعض المؤسسات حيث يسمح فيها للمستخدمين باستخدام أجهزتهم الشخصية في مجال العمل

مضاد الفايروسات: Anti-Virus

برنامج صمم لكشف وحذف الفايروسات ومختلف البرامج الخبيثة الأخرى

معيار التحقق الثنائي: Two factor authentication

هي طبقة أمان إضافية حيث يتم توثيق حسابه المستخدم باستخدام عاملين بدلا من استخدام عامل واحد

الجدار الناري: Firewall

هو جهاز أو برنامج يتم استخدامه لوضع مجموعة من القواعد و القوانين, و التي تستخدم لتقييد اتصالات الشبكة بغرض منع أي اتصال صادر أو وارد غير مصرح به

الإدراج في القائمة البيضاء: Whitelisting

التصريح لبرامج محددة بالعمل دون أخرى على الأنظمة المراد حمايته. تبني هذه الطريقة يعمل على زيادة أمان الأنظمة حيث إنها لا تسمح بتشغيل أي برنامج آخر غير مصرح له بالعمل

الترميم: Patching

عملية إضافة التحديثات إلى الأنظمة أو البرامج المستخدمة بغرض تطوير الجوانب الأمنية و الوظيفية الخاصة بها

البصمة الرقمية: Digital Footprint

هي المعلومات المتعلقة بالمستخدم التي قد يتركها خلفه نتيجة لأنشطته عبر الانترنت وغالبا ماتكون بدون علمه

التشفير: Encryption

وهي عملية تحويل المعلومات إلى صيغة مبهمة غير مقروءة لأحد باستثناء من يملك المفتاح الخاص الذي يمكن استخدامه لإعادة تحويل المعلومة المشفرة إلى صيغتها المقروءة

المنطقة منزوعة: Demilitarized Zone

هي شبكة فرعية من الشبكة المحلية وغالبا ماتكون محمية بجدار ناري ويوضع فيها الخوادم التي تحتوي خدمات يمكن الوصول إليها من الأنترنت

مضاد هجمات حجب الخدمة: Anti-DDOS

أداة تعمل على منع هجمات حجب وتعطيل الخدمة والتي يقوم خلالها شبكة من الأجهزة بمهاجمة خادم واحد بغرض تعطيل خدماته

مصيدة العسل: Honeypot

إحدى استراتيجيات الدفاع التي تعتمد على خداع المهاجمين بوضع جهاز مستقل يحتوي على معلومات مزيفة وغير حقيقية بغرض تمويه المهاجمين وإيقاعهم في الفخ

إعداد:
ندى الرحيلي @Nada_Alruhaily
سعود العتيبي goo.gl/xDcAe9
د. ياسر هوساوي @yaser_hawsawi
ماجدة وزان @majda_wazzan

تصميم:
أيمن الفاضل @afaddhel

تدقيق لغوي:
أسامة الرويلي @osamaalruwaili

HemayaGroup

#وعيك_سبيل_أمنك

مصطلحات في

الهجمات الإلكترونية

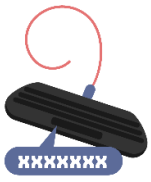
CYBER ATTACK
الهجوم الإلكتروني

هجوم إلكتروني لمحاولة تعطيل أو إلحاق الضرر بالأجهزة والشبكات أو الدخول غير الشرعي على الأنظمة والتنصت عليها

ZERO-DAY VULNERABILITIES
ثغرات يوم الصفر

و يطلق هذا المصطلح على الثغرات التي يتم اكتشافها مؤخرا و لم تعرفها شركات الحماية بعد. يمكن استخدام مثل هذه الثغرات لاختراق الأنظمة المتضررة و إلحاق الضرر بها قبل توفير الحماية المناسبة لها

KEY-LOGGER
مسجل المدخلات عبر لوحة المفاتيح



عبارة عن جهاز يتم وضعه في مخرج لوحة المفاتيح أو برنامج رقمي من أجل تسجيل كل ما يدخله المستخدم عبر لوحة المفاتيح

MACRO
ماكرو

يستخدم للتعبير عن دمج عدة أوامر - و التي غالبا مايتكرر استخدامها - في أمر أو برنامج واحد بسيط يمكن استخدامه بسهولة في بعض البرامج مثل (المايكروسوفت وورد) يمكن استخدام الماكرو أيضا من قبل المخترقين بغرض تنفيذ مجموعة من الأوامر الخبيثة في النظام

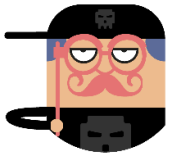
BOTNET
بوت نت

شبكة من الأجهزة المصابة متصلة عن طريق الإنترنت، تستخدم لشن هجمات إلكترونية موسعة بواسطة المخترق دون علم صاحبها

DOS
حجب الخدمة

نوع من الهجمات الإلكترونية على الشبكة او الخدمات الإلكترونية تهدف إلى منع وصول المستخدمين إلى هذه الخدمات عن طريق إغراق الخادم بكمية كبيرة من الطلبات المزيفة

SOCIAL ENGINEERING
الهندسة الاجتماعية

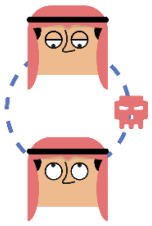


إستخدام الأساليب اللفظية أو النفسية أو الإيحائية أو الإعلانية للتأثير على الضحية للكشف عن معلومات شخصية أو سرية دون أن يشعر لاستخدامها لأغراض الاحتيال

SPOOFING
الاحتيال

عملية احتيال يقوم بها المهاجم للمحاولة للوصول لنظام المستخدم أو الحصول على معلومات حساسة عن طريق التظاهر بكونه مستخدم شرعي أو من مصدر موثوق كتزييف البريد الإلكتروني أو عنوان بروتوكول الانترنت

MAN IN-THE-MIDDLE
الرجل في المنتصف



نوع من أنواع الهجمات التي يقوم فيها المهاجم باعتراض خط التواصل بين طرفين للتنصت أو تغيير المعلومات المتبادلة بينهم

SPEAR PHISHING
التصيد الموجه

هو نوع من التصيّد يتم فيه إرسال الرسائل البريدية بشكل مدروس و غير عشوائي بحيث تبدو الرسالة و كأنها مرسلة من شخص معروف و موثوق

PHISHING
التصيّد

إرسال رسائل إلكترونية مخادعة لعدد كبير من المستخدمين بدون استهداف فئة محددة تطلب منهم إدخال بيانات حساسة (مثل بيانات الحساب البنكي أو كلمة المرور أو تحديثهما) أو تطلب منهم زيارة مواقع إلكترونية مزيفة

WHALING
تصيد الحيتان

و تشير إلى هجمات التصيد التي تستهدف كبار المسؤولين في شركة ما بغرض الحصول على الكم الهائل من المعلومات القيمة جداً و التي تمثل كنزاً ثميناً لدى المخترقين

إعداد
ندى الرحيلي @Nada_Alruhaily
سعود العتيبي goo.gl/xDcAe9
د. ياسر هوساوي @yaser_hawsawi
ماجدة وزان @majda_wazzan

تدقيق لغوي
يزيد التميمي @Yazeedst

تصميم
لينة المسلم @Lenahdaij

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup

#وعيك_سبيل_أمنك

مصطلحات في البرمجيات الخبيثة

البرمجيات الخبيثة (Malware)

هي برمجيات يتم تسريبها إلى أجهزة الحاسب الآلي دون علم ملاكها وبدون الحصول على إذنٍ منهم بغرض تحقيق أهداف خبيثة.

برمجيات التجسس (Spyware)

هي برمجيات تعمل خلف الكواليس في أجهزة الحاسب الآلي دون علم ملاكها للتجسس ونقل معلومات من الأجهزة المصابة.

برمجيات نشر الدعاية والإعلان (Adware)

هي برمجيات تعمل في الخفاء داخل أجهزة الحاسب الآلي لمعرفة اهتمامات الملاك ومن ثمّ إرسال مواد دعائية وإعلانية ضمن تلك الاهتمامات .

برمجيات الفدية (Ransomware)

هي برمجية خبيثة تعمل على جعل البيانات والأنظمة مشفرة أو غير صالحة للاستخدام، ومن ثم يطلب من الضحية دفع مبلغ مالي مقابل إرجاع الأنظمة والبيانات إلى وضعها الطبيعي.

حصان طروادة (Trojan)

هو نوع من البرمجيات الخبيثة و التي غالباً ما يتم تقديمها كبرمجيات مشروعة و غير ضارة و ذلك بغرض خداع المستخدم و دفعه لتحميلها ، وبعد التحميل يتم استخدام هذا النوع من البرمجيات من قبل المخترقين للدخول الغير مصرح به إلى أنظمة المستخدمين.

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup

إعداد:
ندى الرحيلي @Nada_Alruhaily
سعود العتيبي goo.gl/xDcAe9
د. ياسر هوساوي @Yaser_hawsawi

تصميم:
وفاء الداود @Wafa_Aldawoud
تدقيق لغوي:
نوره الطليان @Noorasaadtulaia

#وعيك_سبيل_امنك

الخصوصية

استخدام الإنترنت أصبح من العادات التي لايمكن الاستغناء عنها عند الكثير، ولكن كيف يمكن الاستمتاع بما تقدمه خدمات الإنترنت مع المحافظة على قدر كبير من الخصوصية في الوقت نفسه؟

فيما يلي بعض المخاطر والتوصيات التي ينصح بأخذها في عين الاعتبار لضمان الحماية الكافية للخصوصية

المخاطر

الهوية الرقمية

لكل مستخدم إنترنت متصل بالشبكات الاجتماعية هوية رقمية. وهي عبارة عن ملف شخصي يحتوي على كل ما يقوم المستخدم بنشره على الإنترنت كالكلمات الدلالية المدخلة في محركات البحث والمحادثات الخاصة وعناوين الIP وعناوين المواقع التي تمت زيارتها والتي يتم وضعها في أرشيف عن طريق بعض المؤسسات التجارية والمشبوهة بهدف استغلالها لأغراض تجارية وأخرى ضارة

استخدام حسابات التواصل الاجتماعي للتحقق من السلوكيات

العديد من المؤسسات تقوم بالتحقق من سلوكيات المتقدمين للوظائف وتوجهاتهم عن طريق فحص أنشطتهم من خلال حساباتهم في وسائل التواصل الاجتماعية

انتحال الشخصية

تداول المستخدم لمعلوماته الحساسة كرقم الهوية الوطنية أو تاريخ الميلاد على الإنترنت قد يفتح الباب أمام خطر انتحال هويته

المضايقات الإعلانية

تقوم بعض شركات الإعلانات بتوظيف المعلومات الشخصية للمستخدمين المنشورة على الإنترنت لتوجيه الإعلانات غير المرغوب بها للمستخدمين سواء عن طريق الإيميل أو المتصفح

التوصيات

كن حذرا من شبكات الواي فاي العامة

تجنب إجراء المعاملات المالية وتداول المعلومات الحساسة عن طريق شبكات الواي فاي العامة أو على أجهزة الكمبيوتر العامة وتذكر أنه يلزم تسجيل الخروج من حساباتك عند الانتهاء من جلسة العمل

تحكم في مستوى ظهورك على الإنترنت

أعد تعيين إعدادات الأمن والخصوصية على جميع خدمات الويب والأجهزة والتطبيقات والحسابات عبر الإنترنت إلى مستوى مقبول في نظرك لتبادل المعلومات

ماذا تنشر على شبكات التواصل الاجتماعي

كن حذرا جدا عند مشاركة المعلومات عنك أو عن الآخرين في حسابات التواصل الاجتماعي مثل (عنوان المنزل وتاريخ الميلاد ومشاركة المواقع وما إلى ذلك

فكر قبل أن تتصرف

احذر من رسائل البريد الإلكتروني التي تطالبك بتقديم معلومات شخصية على الفور، أو تحاول إغراءك للقيام بأعمال قد تكون ضارة على جهازك كفتح الروابط أو المرفقات المشبوهة

تمكين معيار التحقق الثنائي

تفعيل معيار التحقق الثنائي لزيادة تحصين حساباتك الرئيسية والمهمة كالبريد الإلكتروني، وحسابات وسائل التواصل الاجتماعي

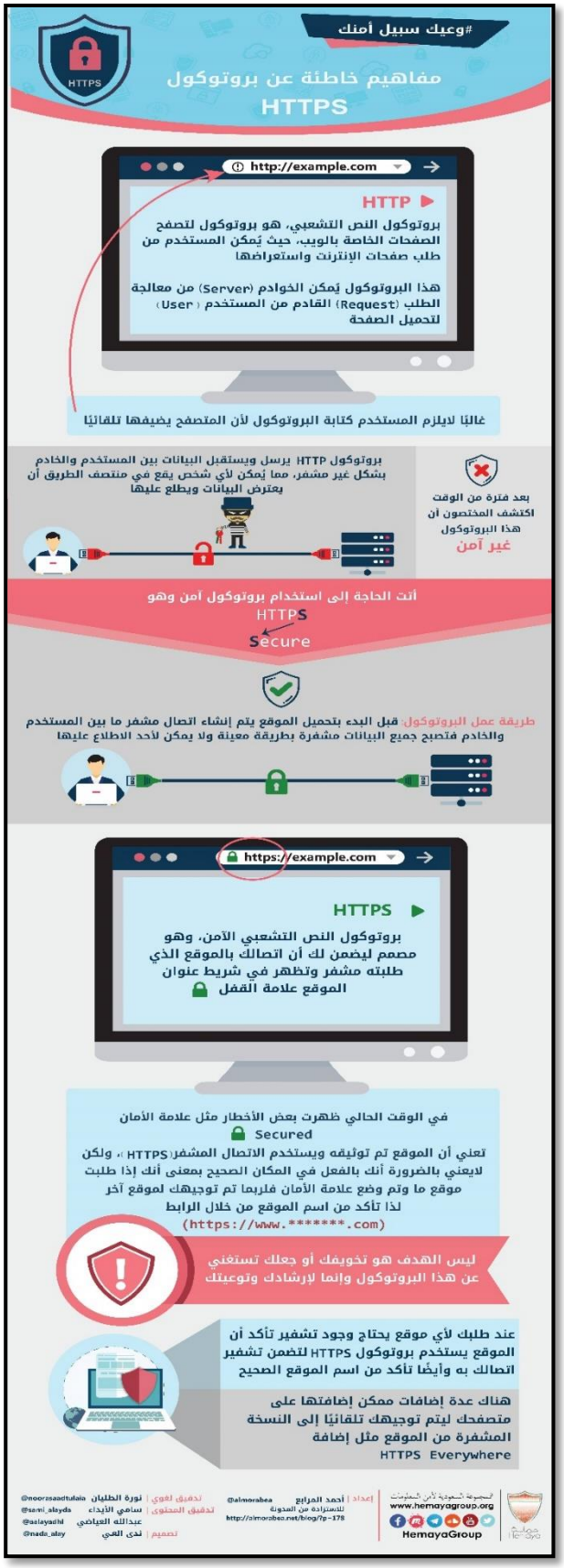
المواد التي تقوم بنشرها يمكن أن تستمر مدى الحياة

قبل نشرها عبر الإنترنت، فكر في الطريقة التي يمكن أن يُنظر إليها الآن وفي المستقبل، ومن الأشخاص الذين قد يرون ذلك الآن وفي المستقبل أيضاً

حذف أي حسابات قديمة لم تعد تستخدمها

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup

إعداد : سعود العتيبي goo.gl/xDcAe9
تصميم: سماهر العرابي @i_smaher
تدقيق :عبدالله العياضي @aalayadhi


#وعيك سبيل أمنك
مفاهيم خاطئة عن بروتوكول
HTTPS
http://example.com
HTTP
بروتوكول النص التشعبي، هو بروتوكول لتصفح الصفحات الخاصة بالويب، حيث يُمكن المستخدم من طلب صفحات الإنترنت واستعراضها
هذا البروتوكول يُمكن الخوادم (Server) من معالجة الطلب (Request) القادم من المستخدم (User) لتحميل الصفحة
غالبًا لايلزم المستخدم كتابة البروتوكول لأن المتصفح يضيفها تلقائيًا
بروتوكول HTTP يرسل ويستقبل البيانات بين المستخدم والخادم بشكل غير مشفر، مما يُمكن لأي شخص يقع في منتصف الطريق أن يعترض البيانات ويطلع عليها
بعد فترة من الوقت اكتشف المختصون أن هذا البروتوكول
غير آمن
أنت الحاجة إلى استخدام بروتوكول آمن وهو
HTTPS
Secure
طريقة عمل البروتوكول: قبل البدء بتحميل الموقع يتم إنشاء اتصال مشفر ما بين المستخدم والخادم فتصبح جميع البيانات مشفرة بطريقة معينة ولا يمكن لأحد الاطلاع عليها
https://example.com
HTTPS
بروتوكول النص التشعبي الآمن، وهو مصمم ليضمن لك أن اتصالك بالموقع الذي طلبته مشفر وتظهر في شريط عنوان الموقع علامة القفل
في الوقت الحالي ظهرت بعض الأخطار مثل علامة الأمان
Secured
تعني أن الموقع تم توثيقه ويستخدم الاتصال المشفر HTTPS ، ولكن لايعني بالضرورة أنك بالفعل في المكان الصحيح بمعنى أنك إذا طلبت موقع ما وتم وضع علامة الأمان فلربما تم توجيهك لموقع آخر لذا تأكد من اسم الموقع من خلال الرابط
(https://www.*******.com)
ليس الهدف هو تخويفك أو جعلك تستغني عن هذا البروتوكول وإنما لإرشادك وتوعيتك
عند طلبك لأي موقع يحتاج وجود تشفير تأكد أن الموقع يستخدم بروتوكول HTTPS لتضمن تشفير اتصالك به وأيضًا تأكد من اسم الموقع الصحيح
هناك عدة إضافات ممكن إضافتها على متصفحك ليتم توجيهك تلقائيًا إلى النسخة المشفرة من الموقع مثل إضافة
HTTPS Everywhere
إعداد | أحمد المرابع @almorabea
للاستزادة من المدونة
http://almorabea.net/blog/?p=178
تدقيق لغوي | نورة الطلبان @noorasaadtulaia
تدقيق المحتوى | سامي الأيداء @sami_alayda
عبدالله العياضي @aalayachi
تصميم | ندى الغني @nada_alay
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup


نقاط مهمة
للحفاظ على الخصوصية الرقمية
للمنظمات من قبل موظفيها
عدم استخدام الأجهزة التقنية التابعة للمنظمة كأجهزة الحاسب الآلي لتنزيل وتنصيب البرامج التي ليس لها علاقة في بيئة العمل
ضرورة الحفاظ على معلومات الدخول وعدم إفشائها أو الإفصاح عنها لأي شخص
عدم استخدام أجهزة خارجية أو شخصية داخل المنظمة إلا بتصريح من إدارة أمن المعلومات
تصريح
التأكد من عدم وجود أشخاص غير مخوّلين للحصول على المعلومات المعروضة في محيط شاشة الحاسب الآلي، مع أهمية تفعيل خاصية شاشة التوقف
عدم نقل الملفات والمستندات التي تخص المنظمة خارج نطاقها -خاصة السرية منها- مهما اختلفت الوسائل والطرق والآليات
استخدام البريد الإلكتروني الخاص بالعمل في نطاق المهام المناطة فقط
التأكد من أن رسائل البريد الإلكتروني صادرة من أشخاص وجهات معروفة أو موثوقة، مع ضرورة فحص الملفات المرفقة قبل فتحها
التواصل مع وحدة أمن المعلومات أو الدعم الفني مباشرة في حال الشك في أي سلوك تقني غير عادي
إعداد: د. ياسر هوساوي
تدقيق: نوره الطليان
تصميم: ريم حميد
@yaser_hawsawi
@noorasaadtulaia
@ReemHamaid
@HemayaGroup
www.Hemayagroup.org

الجزء الأول

الأمان والخصوصية في حسابات تويتر

يعد تويتر أحد الشبكات الاجتماعية الأكثر شعبية والأكثر سهولة والتي تسمح لنا بالتدوينات القصيرة أو "التغريدات" التي تعبر عن أفكارنا و آرائنا. كما يسمح لملايين من المستخدمين بقراءة هذه التغريدات والتعليق عليها و متابعة حسابات الآخرين و معرفة ما يغردون به. كما يعد تويتر بمثابة منصة ضخمة يعتمد عليها للتسويق وبناء السمعة للأعمال الصغيرة والكبيرة وأيضا للمؤسسات المتخصصة مثل الجامعات و الهيئات الحكومية، مما يجعل هذه الحسابات مستهدفة بعدد من المخاطر. إليك أهم النصائح التي تساعدك على تعزيز الأمن والخصوصية لحسابك.

استخدم كلمة مرور قوية وفريدة

استخدامك لكلمة مرور موحدة لحساباتك على الشبكات الاجتماعية أو الخدمات الإلكترونية سيعرّض كل حساباتك للاختراق في حال تم اختراق أحدها. (ينصح بكلمة مرور مكونة من ١٢ خانة تحتوي على احرف كبيرة وصغيرة وأرقام بالإضافة إلى رموز خاصة)

تحكم بالمحتوى الترويجي

يقوم تويتر بمطابقة حسابك مع المعلومات التي توفرها شركات الإعلانات من أجل تخصيص الإعلانات بحسب اهتماماتك، يمكنك إيقاف هذه الخاصية (Setting and Privacy > Privacy and Safety > Promoted Content)
(الإعدادات والخصوصية > الأمان والخصوصية > محتوى مُروَّج)

تجنب إعلان الموقع الجغرافي

تضمين الموقع الجغرافي مع التغريدات قد لا يفيدك بقدر ما يمكن أن يشكل خطرا على خصوصيتك وسلامتك
(Setting and Privacy > Privacy and Safety > Tweet Location)
(الإعدادات والخصوصية > الأمان والخصوصية > تغريد الموقع الجغرافي)

افحص الروابط قبل الضغط عليها

بعض التغريدات تحتوي على روابط مختصرة قد تقودك إلى صفحات مزيفة و إلى الإصابة بالبرمجيات الخبيثة، يمكن تفحصها عن طريق استخدام المواقع الخاصة لذلك

راجع قابلية الاكتشاف بواسطةالبريد الإلكتروني أو الهاتف

إيقاف هذه الخاصية سيمنع الآخرين من الوصول إلى حسابك عندالبحث عنك باستخدام بريدك الإلكتروني أو رقم الهاتف
(Setting and Privacy> Privacy and Safety> Discoverability)
(الإعدادات والخصوصية > الأمان والخصوصية > قابلية الاكتشاف)

تجنب استخدام التغريد الآلي

استخدامك لبرامج التغريد الآلي أو التلقائي سيعرّض صلاحيتك على تويتر للخطر

إعداد: ماجدة وزان @majda_wazzan
تدقيق لغوي: أسامة الرويلي @osamaalruwaili
تصميم: وفاء الداود @wafa_aldawoud

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup

الجزء الثاني

الأمان والخصوصية في حسابات تويتر

فعّل التحقق الثنائي

عند تفعيلك التحقق الثنائي، سيصل جوالك رمز تحقق في كل مرة يتم الدخول إلى حسابك من جهاز مختلف، ففي حال تم تخمين كلمة المرور الخاصة بك ستظل هناك خطوة رمز التحقق التي ستمنع الوصول لحسابك

(Setting and Privacy> Account >Security> Login Verification)

(الإعدادات والخصوصية > الحساب> الأمان> توثيق تسجيل الدخول)

التحقق قبل إعادة تعيين كلمة المرور

يمكن إضافة خاصية التحقق باستخدام معلومة شخصية عند طلب إعادةتعيين كلمة المرور مثل التحقق من رقم الجوال بدلًا من الاكتفاء باسم المستخدم والبريد الالكتروني

(Setting and Privacy> Account> Security> Password Reset)

(الإعدادات والخصوصية> الحساب> الأمان> إعادة تعيين كلمة المرور)

استخدام النماذج الخاصة بالتهديد وانتحال الشخصية

في حال تعرضت لتهديد أو مضايقات أو انتحال للشخصية عبر تويتر لاتتردد في استخدام النماذج الخاصة التي أنشأها تويتر لهذا الغرض، علما بأن القانون يعد ذلك ضمن الجرائم المعلوماتية

كن حريصًا فيما تنشره

إن كل ماتنشره عبر تغريداتك بما في ذلك من معلومات شخصية قد يستخدم ضدك في وقت ما، فكن معتدلًا في تغريداتك

غرّد لأصدقائك فقط

قد يفضل البعض حصر تغريداتهم في وسط معين من الأصدقاء لمزيد من الخصوصية، يمكنهم ذلك

(Setting and Privacy > Privacy and Safety > Tweet privacy)

(الإعدادات والخصوصية > الأمان والخصوصية> خصوصية التغريد)

راجع قائمة التطبيقات التي يمكنها الوصول إلى حسابك

من الممكن أنك قمت بالسماح لبعض التطبيقات بالوصول إلى حسابك بدون قصد مثل تطبيقات الصور أو المحادثات، مما قد يعرض بياناتك للخطر

(Setting and Privacy> App > Revoke Access)

(الإعدادات والخصوصية> التطبيقات> إلغاء الوصول)

تأكد من استخدام التطبيق الأصلي لتويتر

إذا كنت تستخدم تويتر عن طريق الجوال تأكد من أنك تستخدم التطبيق الأصلي لتويتر حتى لا تقع ضحية للتطبيقات المزيفة

إعداد: ماجدة وزان
@majda_wazzan

تدقيق لغوي: أسامة الرويلي
@osamaalruwaili

تصميم: وفاء الداود
@wafa_aldawoud

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup

عناصر التحكم الرئيسية لحماية المؤسسات

SANS Top 20 Critical Controls

1 حصر الأجهزة المصرح بها وغير المصرح بها

إدارة فعالة (حصر، تتبع وتصحيح) لجميع الأجهزة المرتبطة بالشبكة بحيث يتم إعطاء صلاحية الوصول للأجهزة المصرح لها فقط ويتم تحديد الأجهزة غير المصرح بها وغير المدارة ومنعها من الوصول

2 حصر البرامج المصرح بها وغير المصرح بها

إدارة فعالة (حصر، تتبع وتصحيح) لجميع البرامج المرتبطة بالشبكة بحيث يتم السماح بتثبيت و تنفيذ البرامج المصرح بها فقط ويتم تحديد البرامج غير المصرح بها وغير المدارة ومنعها من التثبيت أو التنفيذ

3 تهيئة الإعدادات الخاصة بالأمان لجميع الأجهزة والبرامج (الأجهزة النقالة،المحمولة، الشخصية والخادمات)

إنشاء وتطبيق (تتبع، إبلاغ وتصحيح) إعدادات الأمان الخاصة بالأجهزة المحمولة، الشخصية والخادمات المركزية بإدارة إعدادات الأمان والتحكم في عمليات التغيير بهدف سد ثغرات التطبيقات والأنظمة أمام الهجمات

4 التقييم المستمر ومعالجة الثغرات

تحديث المعلومات الخاصة بالثغرات الجديدة وبشكل مستمر وتقييمها واتخاذ القرارات بهدف التعرف على نقاط الضعف الجديدة وتقليص الفرص أمام الهجمات الإلكترونية

ترجمة

سعد القحطاني @Alabdulwahida
عبدالواحد العبدالواحد https://goo.gl/R7yMmZ

تدقيق لغوي

يزيد التميمي @yazeedst

تصميم

ريهام بارجاء @Re_A_B

المصدر:
https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup

#وعيك_سبيل_أمنك

عناصر التحكم الرئيسية لحماية المؤسسات

SANS Top 20 Critical Controls

5 الاستخدام المقنن للامتيازات الإدارية

تتبع، تقنين، منع وتصحيح استخدام الامتيازات الإدارية و منحها و إعدادها على أجهزة الحواسيب والشبكات والتطبيقات

6 الصيانة، الرصد، و التحليل لسجلات التدقيق

جمع، إدارة وتحليل سجلات التدقيق للأحداث التي يمكن أن تساعد في كشف، فهم أو التعافي من الهجوم الإلكتروني

7 حماية البريد الإلكتروني والمتصفح

التقليل من كمية ومستوى الهجمات الإلكترونية وفرص المخترق في استغلال السلوك البشري من خلال التعامل مع أنظمة البريد الإلكتروني والمتصفح

8 أساليب الدفاع ضد البرامج الخبيثة

التحكم في تنزيل ، نشر، وتنفيذ البرمجيات الخبيثة على مستويات متعددة في المنظمة والبحث عن أفضل الحلول لتفعيل وسائل دفاعية وجمع المعلومات واتخاذ الإجراء السليم

ترجمة

ماجدة وزان @majda_wazzan

سلطان الأسمري @sultandb

تدقيق لغوي

أسامة الرويلي @osamaalruwaili

تصميم

ريهام بارجاء @Re_A_B

المصدر:
https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

عناصر التحكم الرئيسية لحماية المؤسسات

SANS Top 20 Critical Controls

٩ التحكم في منافذ الشبكة والبروتوكولات والخدمات

إدارة (متابعة/ تحكم/ تصحيح) الإستخدام المستمر لمنافذ الشبكة والبروتوكولات والخدمات على مستوى الأجهزة المرتبطة بالشبكة للتقليل من الثغرات الممكن استغلالها من المخترق

١٠ القدرة على استرجاع البيانات

توفر الأدوات والإجراءات المناسبة لعمل نسخة احتياطية للمعلومات السرية و المهمة بطرق موثوقة ومجربة لاستعادتها في الوقت المناسب

١١ إعدادات آمنة لأجهزة الشبكة مثل الجدران النارية، الموجهات، والمفاتيح

إنشاء وتنفيذ وإدارة (تتبع أو تقديم التقارير أو تصحيح) إعدادات الأمان لأجهزة البنية التحتية للشبكة باستخدام إدارة صارمة للإعدادات وعملية التحكم بالتغيير من أجل منع المهاجمين من استغلال نقاط الضعف المُحتملة في الخدمات والإعدادات

١٢ الدفاع عن الحدود

كشف أو منع أو تصحيح تدفق البيانات المنتقلة عبر الشبكة من المستويات الموثوقة المختلفة والتركيز على البيانات الضارة والمدمرة

ترجمة

سلطان الأسمري @sultandb

ماجدة وزان @majda_wazzan

حسناء الشمري @hass_fsh

تدقيق لغوي

عبدالله العياضي @aalayadhi

تصميم

ريهام بارجاء @Re_A_B

المصدر:
https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

عناصر التحكم الرئيسية لحماية المؤسسات

SANS Top 20 Critical Controls

13 حماية البيانات

منع النقل غير المصرح للبيانات، التقليل من آثار البيانات المنقولة بغير تصريح والتأكد من خصوصية وسلامة المعلومات الحساسة

14 التحكم بالوصول بناء على الحاجة إلى المعرفة

تتبع، تحكم، امنع، صحح، وقم بتأمين الوصول إلى الأصول الهامة والحساسة كالمعلومات والأنظمة، بناءً على التحقق الرسمي للأشخاص أو الأجهزة أو التطبيقات التي تحتاج إلى الوصول إلى تلك الأصول بناء على التصنيف المعتمد

15 التحكم بالوصول اللاسلكي

تتبع، تحكم، امنع، وصحح أمان الاتصال اللاسلكي للشبكة المحلية ونقاط الوصول والأنظمة المتصلة بها

16 مراقبة و ضبط الحساب

أدر بشكل فعال دورة حياة حسابات النظم و التطبيقات - إنشاءها، استخدامها، تعطيلها، إلغاءها - لتقليل فرص أستغلالها من قبل المهاجمين

ترجمة

حسناء الشمري @hass_fsh

حامد الكاف @hamidhossain

حسين الجحدلي @haljahdali

تدقيق لغوي

أسامة الرويلي @osamaalruwaili

تصميم

ريهام بارجاء @Re_A_B

المصدر:
https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

عناصر التحكم الرئيسية لحماية المؤسسات

SANS Top 20 Critical Controls

17

تقييم المهارات الأمنية والتدريب المناسب لسد الثغرات

حدد المعرفة والمهارات والقدرات اللازمة للدفاع عن المؤسسة ، وتطوير وتنفيذ خطة متكاملة لتقييم وتحديد و معالجة الثغرات من خلال السياسات والتخطيط التنظيمي والتدريب وبرامج التوعية لجميع الأدوار الوظيفية في المنظمة

18

أمن برمجة التطبيقات

أدر دورة حياة أمن برمجة التطبيقات المصممة داخل المؤسسة أو التطبيقات المستحوذ عليها و ذلك لمنع و رصد و تصحيح الثغرات الأمنية

19

الاستجابة لحوادث أمن المعلومات و إدارتها بشكل فعال

لحماية الأصول المعلوماتية للمنظمة و سمعتها، ينبغي تطوير وتنفيذ سياسة للاستجابة لحوادث أمن المعلومات و استخدام الحلول التقنية لذلك (كتابة خطة وتحديد المهام والأدوار ، وتدريب فريق الاستجابة، وعملية التواصل ، والقيام بالإشراف وإدارة الفريق واختبار فعالية الخطة والقدرات)

20

اختبار قابلية المنظمة للاختراق

ينبغي اختبار قدرة (الأنظمة والإجراءات والموارد البشرية) على حماية الأصول المعلوماتية للمنظمة من خلال تمارين و سيناريوهات و محاكاة للمخترقين (الهاكرز)

ترجمة

ماجدة وزان @majda_wazzan

حسين الجحدلي @haljahdali

سامي العنزي @SamiAlanaz1

تدقيق لغوي

أسامة الرويلي @osamaalruwaili

تصميم

ريهام بارجاء @Re_A_B

المصدر:
https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

الأمن السيبراني

في ظلّ التطوّرات التقنيّة الحديثة تم تحويل معظم الأجهزة و الأنظمة من مستقلة بذاتها إلى أنظمة تتم إدارتها و تشغيلها و التحكم بها عن طريق شبكات و أجهزة الحاسب مما جعلها عرضة للاختراقات وللهجمات الإلكترونية المختلفة

يشير **الأمن السيبراني** إلى التقنيات و الممارسات الأمنية المستخدمة بغرض "حماية الشبكات و أنظمة تقنية المعلومات و أنظمة التقنيات التشغيلية، و مكوناتها من أجهزة و برمجيات، و ماتقدمه من خدمات و ماتحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع".(1)

لا يقتصر الأمن السيبراني على حماية المعلومات الإلكترونية و ضمان سريتها و سلامتها و توافرها فقط، بل يتعدى ذلك ليشمل حماية الأنظمة ذاتها من الاستغلال (كأنظمة المراقبة و التحكم)، بالإضافة إلى حماية الخدمات التي يتم تقديمها عن طريق استخدام مثل هذه الأنظمة من التعطيل (كالبنية التحتية)

أمثلة على الأنظمة و الخدمات التي قد تكون هدفاً للهجمات

- الأجهزة الطبية المرتبطة ببرامج خاصة للتحكم بها و متابعتها
- بطاقات و أنظمة الدفع الإلكتروني
- أنظمة المراقبة و التحكم في القطاعات الحيوية
- الأجهزة الذكية المرتبطة بالشبكة و المعتمدة على الحساسات (IOT devices)

أمثلة على الهجمات و الوسائل التي يهدف الأمن السيبراني للحماية منها

- الاختراقات الناتجة عن استغلال الثغرات، و هجمات تعطيل الخدمة.
- الوصول إلى البيانات و استغلالها عن طريق استخدام أساليب التحايل كالهندسة الاجتماعية و التصيد.
- البرمجيات الخبيثة التي تستخدم للتحكم بالأجهزة المصابة، و تعطيلها، أو سرقة المعلومات منها.

و يختلف تصنيف هذه الهجمات باختلاف الغرض الأساسي منها فقد تتفاوت من جرائم إلكترونية ضد أفراد أو مؤسسات إلى حرب إلكترونية ضد دولة بأكملها و ذلك عن طريق تهديد أمن الدولة الوطني و بنيتها التحتية.

إعداد : د.ندى الرحيلي @Nada_Alruhaily
تصميم: سماهر العرابي @i_smaher
تدقيق : نورة الطليان @noorasaadtulaia
علي الشهري @ali_alshehri

(1)مصدر التعريف :الهيئة الوطنية للأمن السيبراني

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup

الأدلة الرقمية

الدليل الرقمي

هو المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية

فهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم من أجل الربط بين الجريمة والمجرم والمجني عليه

تكمن أهمية الأدلة الجنائية بشكل عام و الأدلة الرقمية بشكل خاص في دورها الرئيس في التحقق من وقوع الجريمة المعلوماتية

حجية الأدلة الرقمية في الإثبات

(الدليل الرقمي حجة معتبرة في الإثبات متى سلم من العوارض ويختلف قوة وضعفاً حسب الواقعة وملابساتها وما يحف به من قرائن)

الهيئة العامة للمحكمة العليا
قرار رقم (34) لعام 1439هـ

شروط صحة الدليل الرقمي

- تحديد الجهاز محل الاشتباه المعبر عن سلوك الجاني
- تحديد الجهاز محل الجريمة التي تمت عبره
- توافر الشروط الشكلية والموضوعية والقانونية، والكفاءة الفنية في مستنبط الدليل
- التحقق من وجود فعل إجرامي قد وقع
- تحريز الدليل بشكل صحيح من مسرح الجريمة من قبل المتخصصين
- حفظ الدليل وإرساله لجهة القضاء بشكل آمن

مواصفات الدليل الرقمي

- موثوق
- مقنع
- كامل
- مقروء ومفهوم
- دقة عالية

ماتتميز به الأدلة الرقمية عن الأدلة التقليدية

- إمكانية استرجاع و إظهار الأدلة الرقمية مرة أخرى بشكل كامل أو جزئي بعد محوها وفق ظروف تقنية
- تكونها من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة
- إمكانية استخراج نسخ من الأدلة الرقمية مطابقة للأصل ولها ذات القيمة العلمية والقضائية
- ذات طبيعة فائقة السرعة حيث تنتقل من مكان لآخر عبر شبكات الاتصال
- إمكانية رصد المعلومات عن الجاني وتحليلها حيث يمكن تسجيل حركات الشخص وعاداته وسلوكياته

الجرائم التي يساعد الدليل الرقمي في إثباتها

- الجريمة المعلوماتية التي تنفذ باستخدام التقنية
- الجريمة التقليدية التي تنفذ باستخدام التقنية
- الجريمة التقليدية التي تلعب التقنية دوراً رئيسياً في كشفها

أماكن تواجد الدليل الرقمي

الأماكن الشائعة التي تتواجد فيها الأدلة الرقمية

أهمية تحريز الدليل الرقمي بالطرق المعتمدة دولياً

للمحافظة عليها من التلف أو الضياع أو التعديل لتقديمها للجهات العدلية

إعداد | فريق التوعية بالجرائم الإلكترونية
تدقيق لغوي | عبدالله العياضي @aalayadhi
تصميم | أبرار الرفاعي @AbrarSR

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup


مبـــــــروك!
لقد فزت بجـــــائزة
1
تصل للضحية رسالة مباركة للفـوز بالجـائزة. والرسـالة ركيكـة بـاللغتين العربيـة والإنجليزيـة وتطلـب الاتصال برقم.
2
عند الاتصال، غالباً ما يجيب شخص لا يتقن العربية.
3
لايتجاوب حتى يتم إخباره باسـتقبال رسـالة مفادهـا الفوز بجائزة.
4
مباشرة يطلـب رقـم بطاقـة الأحوال أو الإقامة.
5
ويطلـب اسـم البنـك الـذي يتعامـل معـه الضـحية. وبنـاءً على اسم البنك يقوم بإخبار الضـحية بـأول 4 أرقـام مـن بطاقة السحب الآلي كنوع من التطمـين والإحسـاس بالثقـة ويطلـب رقـم بطاقـة السـحب كاملًا.
6
SMS
وكـذلك يطلـب الرسـالة التـي اسـتقبلها الضـحية علـى جواله.
7
الفكـرة أنـه يقـوم باسـتعادة كلمة المرور كونه يعرف رقم بطاقة الأحوال أو الإقامة ورقم الجوال.
8
عند إعطائـة الـرقم الـذي وصـل علـى الجـوال فقـد حصـل المهـاجم فعليـاً علـى كافـة بيانات الحساب البنكي.
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup
إعداد: عبدالرحمن الهندي A_Alhindi@
تدقيق لغوي: علي الشهري Ali_alshehri@
تصميم: وفاء الداود Wafa_aldawoud@

أمن أنظمة التحكم الصناعي
SCADA

Supervisory Control And Data Acquisition

أنظمة SCADA هي أنظمة الإشراف و التحكم و المراقبة عن بعد لأنظمة التحكم الصناعية بهدف أتمتة عمليات التحكم و التشغيل. وتستخدم بشكل كبير في أغلب المصانع و خطوط نقل البترول و إدارة شبكات المياه و الكهرباء و غيرها. و غالباً ما تختلف معايير الأمن في أنظمة و شبكات SCADA عن البقية بحكم حساسيتها.

الأخطار المحتملة لأنظمةSCADA

- البرامج الخبيثة
- الإرهاب
- الكوارث الطبيعية
- الضوضاء على خطوط الكهرباء
- انقطاع الخدمة
- الأخطاء البشرية
- تعطيل المرافق

أبرز أمثلة اختراقات أنظمة SCADA

2000 — Maroochy Shire (QLD)
أدى اختراق داخلي إلى تسرب 800,000 لتر من مياه الصرف الصحي الخام إلى المنتزهات المحلية والأنهار

2003 — CSX Train Signaling System
أدى انتشار فايروس SoBig إلى انقطاع الإشارات بشبكة القطارات.

2006 — Zotob Worm and Chrysler
أدى انتشار فايروس Zotob إلى إغلاق أكثر من ١٤ مصنعاً

2010 — Stuxnet
انتشار أشهر البرامج الخبيثة التي تستهدف أجهزة Siemens أحد الشركات المصنعة لأنظمة SCADA

تأمين أنظمةSCADA

- تطبيق أفضل المعايير لتأمين شبكة SCADA.
- عزل شبكات أنظمة SCADA عن جميع الشبكات سواء كانت داخلية أم خارجية.
- توفير التشفير اللازم بين الوحدات الطرفية لأنظمة SCADA.
- إجراء اختبارات أمنية و فحص الثغرات بشكل دوري.
- إجراء مراجعة التعليمات البرمجية لوحدات (Programmable Logic Controllers).
- تطبيق سياسة إدارة الحسابات و كلمة المرور.
- التأكد من إجراء جميع التغيرات وفقاً إلى سياسة إدارة التغيير.
- إقفال استخدام الـUSB و منع الوصول إلى الإنترنت.
- توفير حماية مادية بشكل قوي لجميع الوحدات الطرفية لأنظمة SCADA.
- تطبيق و تحديث أنظمة مكافحة الفيروسات على جميع أجهزة SCADA.
- توفير أنظمة مكافحة الفيروسات المدمجة لوحدات الـ (Remote Terminal Unit).
- تحديث الأنظمة وأخذ نسخ احتياطية بشكل دوري.
- مراقبة و تحليل شبكات و أنظمة SCADA بشكل مستمر.
- توفير برامج توعية أمنية لجميع مسؤولي أنظمة SCADA.

إعداد : م . رائد العتيبي @rff_1122
تدقيق لغوي : عبدالله العياضي @aalayadhi
تصميم : شفاء الشهراني @shafya_15
: ماجد الدهمشي @majedsurur

www.hemayagroup.org
HemayaGroup

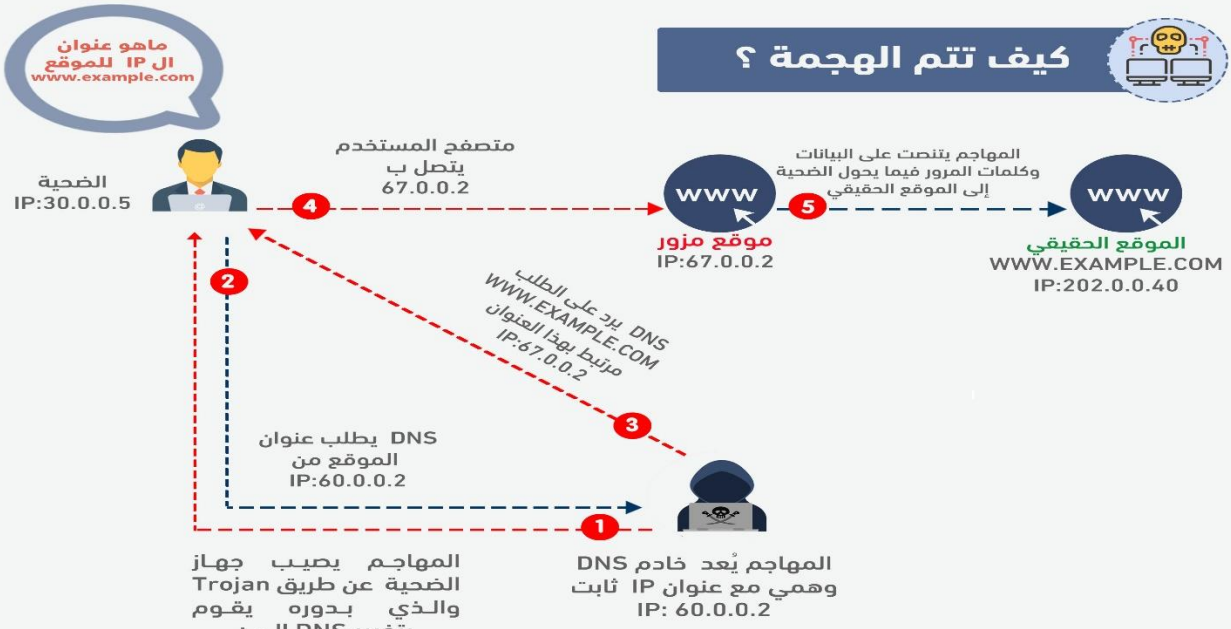

التشفير وأنواعه
ماهو التشفير ؟
هو تحويل النص المقروء إلى نص غير مقروء لأي أحد باستثناء الشخص الذي يملك مفتاح فك التشفير .
ماهو فك التشفير ؟
عملية استخدام المفتاح لإعادة النص المشفر إلى صيغته المقروءة الأصلية.
أهدافه
السرية أوالخصوصية
التكاملية وسلامة البيانات (Integrity)
إثبات الهوية (Authentication)
عدم الإنكار (Non-repudiation)
أنواع التشفير
التشفير الحديث
(Modern Cryptosystem)
وينقسم إلى قسمين :
تعريفه
١- التشفير المتماثل Symmetric Cryptography
يستخدم مفتاحاً واحداً لعملية التشفير وفك التشفير للبيانات . ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدم حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات
٢- التشفير الغير متماثل Asymmetric Cryptography أو التشفير بالمفتاح العام
ويعتمد على وجود مفتاحين هما :
- المفتاح العام (Public Key) و يستخدم لتشفير الرسائل كذلك يرسل لجميع الناس .
- المفتاح الخاص (Privet Key) و يستخدم لفك تشفير الرسائل كذلك يحتفظ به صاحبه ولايرسله لأحد .
فمن يحتاج أن يرسل رسالة مشفرة فإنه يستخدم المفتاح العام للمستقبل لتشفيرها ومن ثم يستقبلها المستقبل ويقوم بفك تشفيرها بمفتاحه الخاص .
التشفير التقليدي
(Classical Cryptosystem)
كان يستخدم في عصر ماقبل الكمبيوتر
يعتمد على أحد أمرين :
١- تبديل الأحرف Substitution
٢- تغيير مواقع الأحرف Transposition
ملاحظة مهمة :
يمكن قياس قوة التشفير بالوقت والمصادر المتطلبة لعملية فك النص المشفر إلى النص الأصلي .
مميزاته
التشفير المتماثل :أسرع في عملية التشفير .
التشفير الغير متماثل :
١- يستخدم مفتاحين في عملية التشفير وفك التشفير و هو أقوى وأقل عرضة للإختراق
٢- يمكن استخدامه للتوقيع الإلكتروني وتوقيع الشهادات الرقمية .
عيوبه
التشفير المتماثل :
١- مشكلة نقل مفتاح التشفير key Distribution مما يجعله قابل للسرقة وكسر التشفير
٢- لايمكن استخدامه للتوقيع الإلكتروني وتوقيع الشهادات الإلكترونية
التشفير الغير متماثل : أبطأ سرعة من التشفير المتماثل
يمكن كسرها في الوقت الحاضر بسهولة مع استخدام الكمبيوتر .
خوارزمياته
التشفير المتماثل :
١- تشفير البيانات القياسي DES
٢- معيار التشفير المطور AES
التشفير الغير متماثل :
PGP,DSA,Deffie-Hellman,Elgamal,RSA
١- خوارزمية القيصر Caeser Cipher .
٢- خوارزمية عامود السياج / أعمدة السياج Rail Fence .
المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
HemayaGroup
حماية Hemaya
إعداد | سجى القرشي @saja_alqurashi
تدقيق علمي | عبدالله القحطاني @ qh_cs
تدقيق لغوي | عبدالله العياضي @aalayadhi + عبدالكريم الإبراهيمي @alberahimi
تصميم | شيماء القحطاني - @shaima2011
المراجع :
Cryptoggraphy and Network Security, 5th Edition, by William

تسميم DNS

(DNS Poisoning)

يستخدم هذا النوع من الهجمات تقنية " الرجل في المنتصف"
(Man - In - The Middle)

كيف تتم الهجمة ؟



توضيح الخطوات

١- يقوم المهاجم بزرع برمجية خبيثة في جهاز الضحية وغالباً ماتكون على هيئة حصان طراودة (Trojan) .

٢- يقوم (Trojan) بتغيير إعدادات خوادم DNS الأساسية الخاصة بالشبكة وتبديلها بخادم آخر معدّ مسبقاً من قبل المهاجم بحيث يمكّنه من الرد على طلبات DNS الخاصة بالضحية .

٣- عندما يحاول الضحية الوصول إلى موقع معين , يقوم المهاجم بتغيير عنوان IP الخاص بالموقع إلى عنوان IP آخر لخادم ضار .

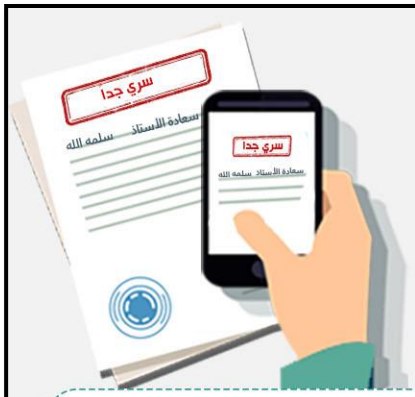
٤- يتصل جهاز الضحية بخادم المهاجم دون أن يدرك ذلك .

٥- يتم تحويل جميع اتصالات الضحية لتمر بخادم المهاجم .

٦- وبذلك يتمكن من التلاعب بجهاز الضحية وتحويل جميع طلبات الوصول لمواقع الويب لأي موقع يريده والتنصت على الكلمات المرورية وكافة البيانات الأخرى .

إعداد | سعود العتيبي Http://goo.gl/xDcAe9
تدقيق لغوي | نوره الطليان @noorasaadtulaia
تصميم | شيماء القحطاني @shaima2011

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org copy
HemayaGroup
حماية Hemaya



" نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها "

(المادة الخامسة)

يُجرم كل من :

- نشر وثائق أو معلومات سرية أو إفشائها.
- دخل أو شرع في الدخول إلى أي مكان أو موقع غير مأذون له الدخول فيه، بقصد الحصول على وثائق أو معلومات سرية.
- حصل بأي وسيلة غير مشروعة على وثائق أو معلومات سرية.
- حاز أو علم - بحكم وظيفته - وثائق أو معلومات رسمية سرية فأفشاها أو أبلغها أو نشرها دون سبب مشروع مصرح به نظاماً.
- أتلف - عمداً - وثائق سرية أو أساء استعمالها وهو يعلم أنها تتعلق بأمن الدولة أو بأي مصلحة عامة، وذلك بقصد الإضرار بمركز الدولة العسكري أو السياسي أو الدبلوماسي أو الاقتصادي أو الاجتماعي.
- أخل بالمحافظة على سرية المعلومات والوثائق.

العقوبة

السجن لمدة لاتزيد عن 20 سنة

أو

غرامة لاتزيد عن مليون ريال

أو

بهما معاً

المصدر: " نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها " المرسوم الملكي رقم م / ٣٥ بتاريخ ١٤٣٢/٥/٨هـ الموافق ٢٠١١/٤/١٢م .
تصميم : شيماء القحطاني @shaima2011
تدقيق لغوي : عبدالله العياضي @aalayadhi

HemayaGroup
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
WWW. HEMAYAGROUP .ORG

منع تسريب البيانات خارج المنظمة

(Data Leakage Prevention)

(Data Leakage Prevention) : هي إحدى استراتيجيات أمن المعلومات والمعنية بالمحافظة على البيانات المهمة والحساسة من الاطلاع غير المشروع ومنع تسربها وتداولها خارج نطاق المنظمة .

طرق تسريب البيانات في المنظمة

- ترك الأجهزة الشخصية بدون تسجيل خروج أو قفل للشاشة.
- الهندسة الاجتماعية لخداع الموظفين واستدراجهم لاستخراج المعلومات السرية منهم.
- الحديث بصوت عالٍ في الأماكن المفتوحة عن ماتحتويه بيانات المنظمة.
- البحث في سلة المهملات عن البيانات المهمة والحساسة.
- استخدام كاميرا الجوال لالتقاط صور للبيانات المهمة والحساسة .
- وصول المخترقين من عالم الإنترنت إلى الشبكة الداخلية للمنظمة.
- سرقة الأجهزة المحمولة والذكية وأجهزة التخزين المتنقلة غير المحمية والتي تحتوي على بيانات مهمة وحساسة .
- التنصت على البيانات المرسلة وغير المشفرة عبر الشبكة الداخلية للمنظمات.
- إرسال البيانات المهمة إلى الخارج عبر البريد الإلكتروني أو تطبيقات المحادثة أو رفعها على مواقع التخزين التجارية.
- ضعف أو غياب أنظمة التحكم بالوصول للتطبيقات وقواعد البيانات والتي عن طريقها يتم الوصول للبيانات المهمة.

طرق حماية البيانات من التسرب

- توعية موظفي المنظمة بالمخاطر الأمنية وتثقيفهم بالسياسات الأمنية وحثهم على اتباعها.
- تصنيف البيانات حسب أهميتها وسريتها وذلك لاتخاذ الإجراء المناسب لكل تصنيف.
- تنظيم صلاحيات الوصول للأنظمة في المنظمة لتكون الصلاحيات وفق الحاجة (Least Privileges).
- مراقبة محتوى الإنترنت والبريد الإلكتروني (Content Inspection) لمنع تسريب البيانات المهمة خارج المنظمة .
- تشفير البيانات المهمة خلال تخزينها أو انتقالها عبر الشبكات لمنع المخترقين من الاطلاع عليها.
- تفعيل أنظمة الحماية على جميع الأجهزة وخدمات الإنترنت والبريد الإلكتروني في المنظمة.
- تقييد أجهزة المستخدمين وفق الحاجة وتعطيل الأجهزة التي قد تساهم في تسريب البيانات مثل (USB/CD/DVD).
- استخدام تقنيات (Mobile Device Management) والتي تعمل على الحفاظ على سرية البيانات المتواجدة على الأجهزة المتنقلة خارج نطاق المنظمة.

Hemayagroup
www.hemayagroup.org
إعداد : سامي الأيداء @sami_alayda
تصميم: شيماء القحطاني @shaima2011
مراجعة وتدقيق لغوي : عبدالله العياضي @aalayadhi

الاستثمار الزائف

من حين لآخر تنتشر دعايات لشركات تزعم أنها تدر للمستثمرين فيها أرباحاً طائلة ويروج منتجو هذه الدعايات لأنفسهم أنهم مندوبين لشركات وساطة ، وعادة يكون زعمهم أنهم يستثمرون في أسواق الفوركس العالمية العقارات ونحوها لذلك يجب الحذر والتأكيد على عدد من الأمور الهامة :

يجب التأكد قبل التفكير في المساهمة مع هذه الشركات أن الفضاء الإلكتروني مليء بالمحتالين الذين يرتكز عملهم على سرقة أموال الناس

يجب البحث دائما عن مصدر موثوق للتأكد من سلامة وضع هذه الشركة أو هذا المعلن بالبحث في الإنترنت عن طريق الجهات الرسمية مثل:هيئة سوق المال و مؤسسة النقد

يجب الحذر دوماً من التعامل مع أشخاص غير معروفين لديك وتغليب جانب الشك على حسن الظن عند التعامل معهم

البعض منهم يملك حسابات في بنوك محلية، لذلك وجود حساب في بنك محلي لا يعني بالضرورة سلامة التعامل مع الطرف الآخر

وجود موقع إلكتروني على الشبكة لايعني بالضرورة أيضا سلامة التعامل، ففكرة إنشاء موقع إلكتروني لاتتعدى مسألة دقائق

يجب عدم الاغترار بالتوصيات التي تظهر في الموقع أو التي يعرضها صاحب النشاط، فلا يوجد ما يثبت صحة هذه التوصيات

يجب عدم التساهل في تحويل أي مبلغ مهما كان لأي شخص افتراضي أو شركة على شبكة الإنترنت

المجموعة السعودية لأمن المعلومات
HemayaGroup
www.hemayagroup.org

إعداد:م.علي عبدالله الشهري
@ali_alshehri

تدقيق لغوي:عبدالكريم البراهيمي
@alberahimi

تصميم:شفياء الشهراني
@shafya_15

المختـرق الداخلي

من هو المخترق الداخلي؟

هو مخترق يعمل داخل المنظمة، ويعتبره أغلب الخبراء أكثر خطورة من المخترق الخارجي.

أهم الأسباب التي يعمل من أجلها المخترق الداخلي

- الرضا الشخصي
- الابتزاز
- الانتقام
- التجسس
- كسب المال

التهديـدات والمخاطـر

1. عمل رسائل تصيدية للحصول على كلمات المرور لمستخدمين لهم صلاحيات عالية على الأنظمة.
2. معرفة وسائل الأمان و الدفاع داخل المنظمة.
3. تحميل برامج التجسس والاختراق بسهولة.
4. عمل مسح شامل للشبكة الداخلية بسهولة.
5. استخدام صلاحية الوصول للدخول على الأنظمة لتجميع البيانات المهمة والحساسة.
6. صعوبة التعرف عليه كونه أحد موظفي المنظمة.
7. إنشاء أجهزة افتراضية VM على جهازه الشخصي للتخفي عن مجال الشبكة.
8. سهولة الوصول لقواعد البيانات وتدميرها وتعطيل الخدمات الإلكترونية للمنظمة.
9. استخدام الهندسة الاجتماعية لخداع زملاء العمل للحصول على معلومات مهمة.

كيف يمكن اكتشافه وإيقافه؟

- ملاحظة أي تصرفات غير عادية.
- مراقبة وتحليل تدفق البيانات على الشبكة.
- مراجعة صلاحيات الوصول للأنظمة و قواعد البيانات.
- مراجعة ملف سجلات Logfile لجميع الأجهزة والأنظمة .
- استخدام برامج و أنظمة متخصصة للحماية و المراقبة.
- استخدام الهندسة العكسية أو المصيدة Honeypot .

إعداد : م.إبراهيم كلنتن @lkalantan

تصميم: سماهر العرابي @i_smaher

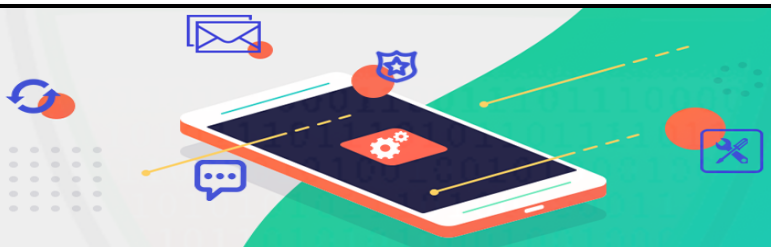
تدقيق: عبدالكريم البراهيمي @alberahimi

المجموعة السعودية لأمن المعلومات

www.hemayagroup.org

@HemayaGroup


#وعيك_سبيل_أمنك
FIFA WORLD CUP
RUSSIA 2018
نصائح للجمهور السعودي
عزيزي المشجع السعودي .. تقدم لك المجموعة السعودية للأمن المعلومات "حماية" نصائح توعوية و نظامية للحفاظ على بياناتك وحقوقك .
تجنب
الشراء من السوق السوداء لضمان حقك كمشجع .
إحرص
على التسجيل في السفارة السعودية.
إحتفظ
بتذاكرك الإلكترونية واحرص على سريتها لإحتوائها على بيانات شخصية.
تأكد
من الإحتفاظ بنسخة من وثائقك في مكان آمن.
تأكد
من وجود حد ائتماني لبطاقتك البنكية مثل (الفيزا).
VISA
تجنب
استخدام الشبكات العامة عند تصفح الإنترنت .
إعداد :
د. متعب الضبيطي
@iMoteeb
تصميم :
شيماء القحطاني
@Shaim2011
تدقيق لغوي :
يزيد التميمي
@yazeedst
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
Hemayagroup
WWW.Hemayagroup.org
حماية



كيف تحمي حساباتك من الاختراق؟

Google

1. من خلال قوقل حسابي
2. تسجيل الدخول و الأمان
3. عملية التحقق بخطوتين
4. ادخل رقمك السري لدخول حسابك
5. ادخل رمز التحقق الذي وصل لجوالك
6. الآن اصبح التحقق بخطوتين فعّال

Apple ID

1. الإعدادات
2. الضغط على اسمك Apple ID
3. كلمة السر و الأمن
4. اضف رقم الجوال الخاص بك
5. ادخل رمز التحقق الذي وصل لجوالك
6. الآن اصبح المصادقة ذات العاملين فعال

Instagram

1. ايقونة الإعدادات
2. اختر Two-Factor Authentication
3. فعّل طلب Security Code
4. ادخل الكود الذي وصل جوالك
5. أصبح لديك أكواد مفعله للاستعادة وتم تصوير الشاشة الياً ومخزنة لديك في ألبوم الصور Translate Tweet

WhatsApp

1. الإعدادات
2. الحساب
3. التحقق بخطوتين
4. تمكين
5. ادخل رقم تعريف
6. ادخل بريد إلكتروني للاستعادة

Telegram

1. الإعدادات
2. الخصوصية والأمان
3. التحقق بخطوتين
4. تعيين كلمة مرور إضافية
5. تعيين بريد إلكتروني للاستعادة
6. الضغط على الرابط الذي وصلك بالبريد

المجموعة السعودية لأمن المعلومات
www.hemayagroup.org
@HemayaGroup

إعداد : راجح بن سالم @RajihSalim

تصميم : سماهر العرابي @i_smaher

التحقق من الهوية

التحقق الرقمي من الهوية :

هو إجراء يتم القيام به إلكترونياً للتأكد من الهوية اعتماداً على إحدَى الوسائل التي يتم الحصول عليها من الشخص بعد تحويلها إلى شكل رقمي.

أنواعه

١- المطابقة

هي عملية التأكد من هوية الشخص عن طريق تطابق الوسيلة التي يقدمها مع ماهو موجود لدى جهة التحقق.

أنواعه

- مايبرزه الشخص كالبطاقات الممغنطة والتوكن
  - المميزات: سهولة الحمل؛ عدم الحاجة للتذكر؛ سهولة الإلغاء وإعادة الإصدار؛ إمكانية التتبع (غير شائع)
  - العيوب: إمكانية التعرض للفقد أو السرقة أو التلف أو التدمير
- مايعرفه الشخص ككلمات المرور وكلمات السر
  - المميزات: عدم الحاجة للحمل؛ سهولة التغيير
  - العيوب: إمكانية التعرض للسرقة أو التغيير في حال إفشائها؛ الحاجة للتذكر

٢- التعرف

هي عملية التأكد من هوية الشخص عن طريق التعرف عليه مباشرة حال تطابق الوسيلة التي لديه مع ماهو موجود لدى جهة التحقق.

أنواعه

- السمات الحيوية كالبصمات والوجه وقزحية العين ورائحة العرق وطريقة المشي
  - المميزات: عدم الحاجة للتذكر؛ عدم الحاجة لحمل أي وسيلة تعريف؛ التعرف على هوية الشخص مباشرة
  - العيوب: عدم إمكانية الإعتماد عليها مستقبلاً في حال انكشافها؛ عدم القدرة على استخدامها لدى البعض (كبار السن والأطفال)؛ تحتاج إلى بيئة وأدوات خاصة
- التعرف على ممتلكات الشخص كجهاز الكمبيوتر والجوال
  - المميزات: عدم الحاجة للتذكر؛ التعرف على الشخص مباشرة؛ تسهيل الدخول إلى التطبيقات
  - العيوب: إمكانية التعرض للفقد أو السرقة أو التلف أو التدمير

٣- التحقق المزدوج (الهجين) :

هي عملية التأكد من هوية الشخص بالاعتماد على الطرق المذكورة أعلاه في نفس الوقت مثل التحقق الثنائي باستخدام كلاً مما يعرفه الشخص وإحدى السمات الحيوية في آن معاً.

آلية التحقق من الهوية

نصائح لحماية وسائل ومعلومات المصادقة الرقمية الشخصية

- أن تكون معتمدة وقوية وسهلة الحفظ والتذكر والاستخدام.
- الحفاظ عليها وعدم مشاركتها مع الآخرين.
- في حال الشك حول احتمالية انكشافها ينبغى إبلاغ المختصين فوراً.
- أي تصرف أو استخدام خاطئ لتلك الوسائل يقع على عاتق مالكها.
- في حال انكشاف السمات الحيوية الشخصية لغير المخولين فمن الصعب الاعتماد عليها في المصادقة.
- تغيير معلومات المصادقة من فترة لأخرى.
- التأكد من الخروج من الأنظمة والتطبيقات قبل مغادرة أماكن تواجد الأجهزة.

إعداد :
د. ياسر هوساوي
@yaser_hawsawi

تصميم :
شيماء القحطاني
@Shaim2011

تدقيق لغوي :
مها القريني
@MQarini

المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance
Hemayagroup
WWW.Hemayagroup.org

5 نصائح
للاستخدام الأمثل للإنترنت

للتأكد من سلامة طفلك على الإنترنت بشكل صحيح إليك بعض النصائح التي يجب اتباعها:

١- راقب أنشطة طفلك على الإنترنت:

كثير من الألعاب غالباً تجذب الطفل إلى غرف الدردشة المدمجة معها (Chat)، والأطفال الأقل من (١٣) سنة أكثر وأسهل تأثراً من غيرهم لذلك تأكد من عدم قيامهم بدخول مواقع محظورة .

٢- كن قريباً من أطفالك وعلى تواصل مستمر معهم:

- تخصيص وقت معين للجلوس معهم وتوعيتهم بكيفية خداعهم على الإنترنت والتأكد من فهمهم للمبادئ الأساسية للفيروسات.
- قم بتشجيع أطفالك على الحديث معك وطمئنهم بأن يخبروك كل شيء بدون خوف.

٣- تأكد من عدم إظهار طفلك لشخصيته الحقيقية على الإنترنت:

يجب إبلاغهم بعدم الكشف عن اسم عائلتهم وعدم توزيع أو نشر أسمائهم أو عنوان المنزل أو كلمة المرور أو رقم الهاتف لأي شخص لايعرفونه.

٤- اجعل حسابات الدخول منفصلة على جهاز الكمبيوتر الخاص بك:

إذا كنت تشارك جهاز الكمبيوتر الخاص بك مع طفلك فامنحه اسم المستخدم الخاص به على جهازك ولاتنس حماية ملفاتك الهامة من حذفها أو توزيعها بدون قصد.

٥- ابلغ أطفالك بالإجراءات الصحيحة لتصفح الإنترنت:

الإنترنت سلاح ذو حدين رائع ومخيف ينجذب إليه الأطفال لذلك لابد من مصارحتهم بالأساليب الخاطئة للتصفح وماذا يجب عليهم فعله ومالايجب أثناء التصفح وعواقبة الحقيقية .

المجموعة السعودية لأمن المعلومات
Hemayagroup
WWW.Hemayagroup.org

إعداد :
م. عبدالإله العضياني
@EngAbdullilah

تصميم :
شيماء القحطاني
@Shaim2011

تدقيق لغوي :
علي الشهري
@ali_alshehri
عبدالكريم البراهيمي
@alberahimi


لا إله إلا الله محمد رسول الله
اللهم احفظ أبطالنا
حماة الدين
حراس الوطن
حماية
Hemaya
@HemayaGroup
www.HemayaGroup.org


اللهم وفق ولاة أمرنا لكل خير
وارزقهم البطانة الصالحة
و اجعلنا عوناً لهم لخدمة هذا البلد
وحمايته
@HemayaGroup
www.HemayaGroup.org
حماية
Hemaya
تصميم @AbrarSR

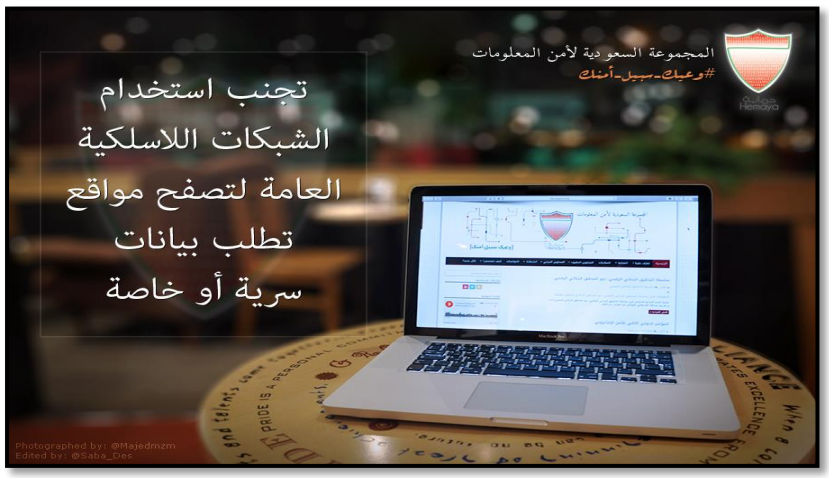

حماية
Hemaya
بايعناك على
السمع والطاعة


حماية
Hemaya
اليوم الوطني
دام عزك ياوطن
HEMAYAGROUP
WWW. HEMAYAGROUP .ORG
Design
INSTA@SAAD698


حماية
Hemaya
محمد بن سلمان بن عبد العزيز آل سعود
"إن مستقبل المملكة مبشر وواعد، وتستحق بلادنا الغالية أكثر مما تحقق. لدينا قدرات سنقوم بمضاعفة دورها وزيادة إسهامها في صناعة هذا المستقبل"
المجموعة السعودية لأمن المعلومات
HemayaGroup
www.HEMAYAGROUP.org
حماية
Hemaya
تصميم
نايف العتيبي


حماية
Hemaya
للمستقبل رؤية واحدة
نجدد البيعة لولي العهد
الأمير محمد بن سلمان
تصميم | ماجد عبدالرحمن العنزي
المجموعة السعودية لأمن المعلومات
HemayaGroup
www.HEMAYAGROUP.org


انسخ ملفاتك
المهمة احتياطياً
على وحدة
تخزين خارجية
@shifaaljuhani
@AbrarSR
HemayaGroup.org
@HemayaGroup


المجموعة السعودية لأمن المعلومات
#وعيك_سبيل_أمنك
تجنب استخدام
الشبكات اللاسلكية
العامة لتصفح مواقع
تطلب بيانات
سرية أو خاصة


تأكد من دوافع
دعوات الإضافة
قبل قبولها
@1316_mysoft
@AbrarSR
HemayaGroup.org
@HemayaGroup


عند الابتعاد عن جهازك
أستخدم خيارات الإغلاق
لتأمينه
إغلاق
تأمين
خروج
@1316_mysoft
@saadAlenazii
HemayaGroup.org
@HemayaGroup


تجنب تنزيل المرفقات من البريد الإلكتروني مجهول المصدر فعادة ما يلجأ المخترقون إلى ارسال ملفات مدمجة ببرمجيات خبيثة من خلال البريد الإلكتروني بهدف سرقة المعلومات الشخصية و السرية للضحية.
يعتبر موقع www.virustotal.com أحد المواقع الفعالة لفحص الملفات للتأكد من خلوها من البرمجيات الخبيثة لتجنب الخطر.
HemayaGroup
WWW. Hemayagroup.org
المجموعة السعودية لأمن المعلومات
Saudi Group for Information Assurance

حماية
Hemaya

@HemayaGroup

www.HemayaGroup.org