دورة تدريبية: حوكمة الأمن السيبراني

الأمن السيبراني في القطاع العسكري

(الجزء الثاني)

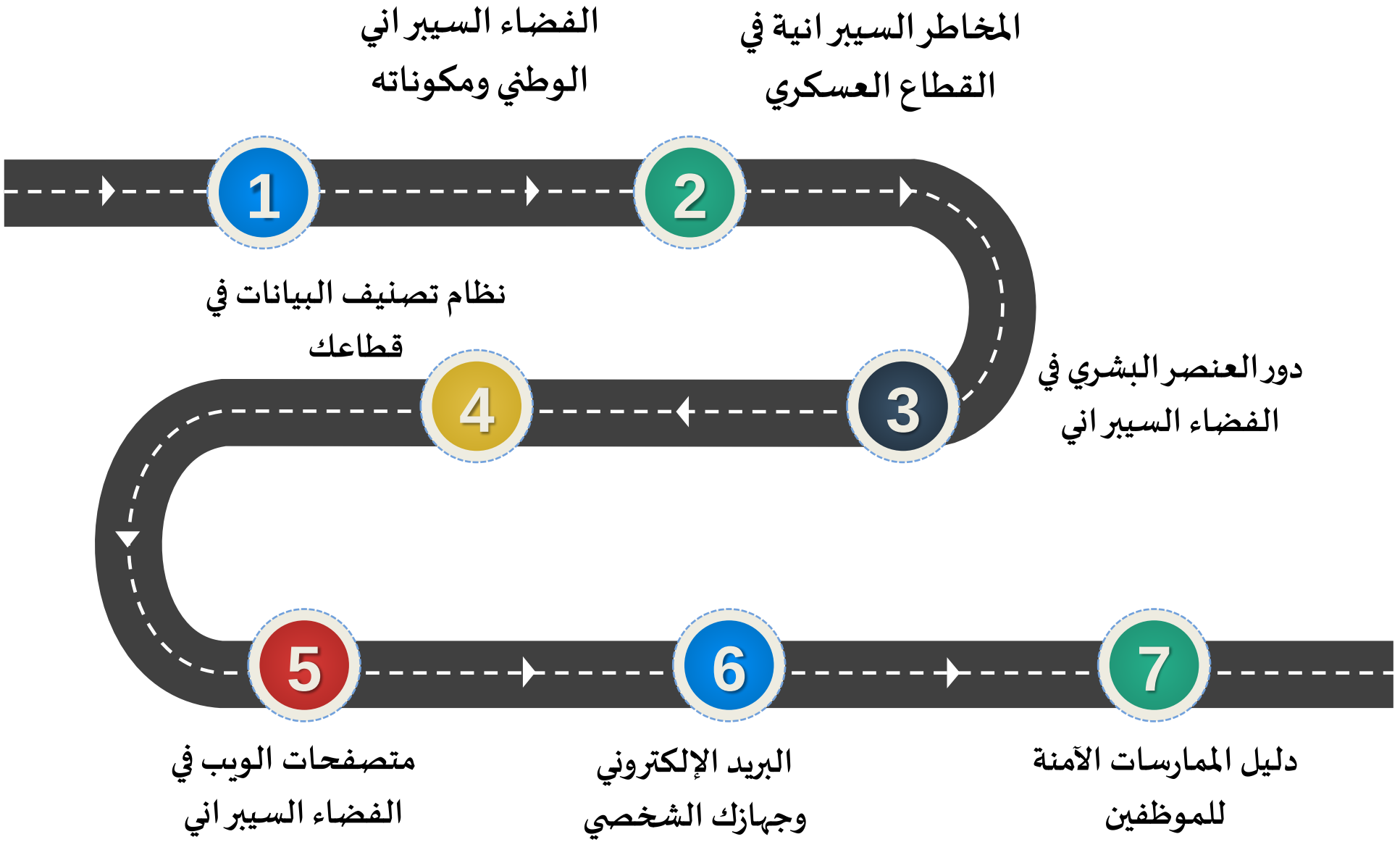
المحاضرة الثالثة

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

خارطة الطريق



عصف ذهني

ما هو مفهوم الأمن السيبراني الوطني وفقاً للأمر الملكي رقم 6801 وتاريخ 11/ 1439/2هـ؟

مفهوم الأمن السيبراني الوطني

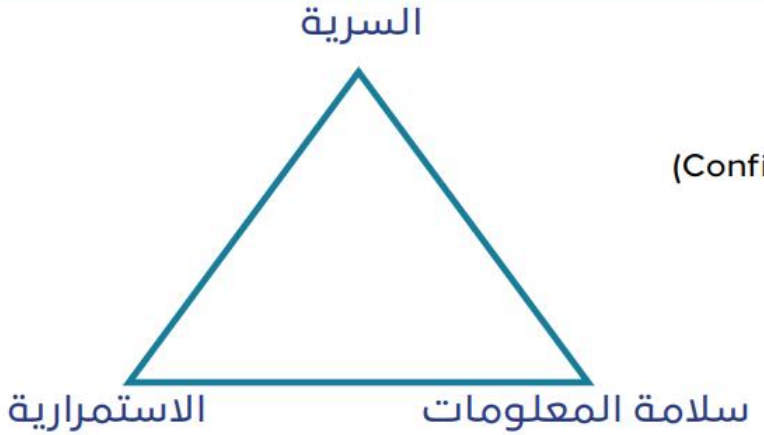
تعريف الأمن السيبراني

"حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك".[1]

مثلث الأمن السيبراني الوطني

مثلث الأمن السيبراني

1. السرية بمفهومها الشامل (للمعلومات والأنظمة والأصول ... وغيرها) (Confidentiality)
2. سلامة المعلومات وضمان مصدرها (Integrity)
3. الاستمرارية وتوفر الأنظمة والمعلومات عند الحاجة لها (Availability)



عصف ذهني

من وجهة نظرك
ما هو مفهوم الهجمات
السيبر انية للقطاع العسكري؟
وما أهدافها؟

الهجمات السيبرانية وأهدافها

يمكن تعريف الهجمات السيبرانية بأنها العبث بأحد ركائز الأمن السيبراني، وهي:

- إفشاء المعلومات العسكرية أو وصول غير المصرح لهم سواء للمعلومات أو الأنظمة أو الشبكات
- العبث بسلامة المعلومات العسكرية أو مصدرها
- تعطيل الأنظمة العسكرية أو منع الوصول للمعلومات وقت الحاجة لها

الهجمات السيبرانية لها العديد من الأهداف العامة والخاصة منها:

- الأهداف التخريبية والتدميرية للأنظمة والبنية التحتية
- أهداف سياسية مثل: الحرب السيبرانية والتجسس السيبراني
- أهداف شخصية مثل نشر المعلومات الخاصة للآخرين وإنتحال الشخصية
- أهداف تجارية ومالية لزعزعة الثقة والمصداقية للمنافسين

عصف ذهني

من وجهة نظرك
ما هي الأساليب المستخدمة في
الجهات للقطاع العسكري؟

الأساليب المستخدمة في الهجمات السيبرانية

- رسائل التصيد الإلكتروني والهندسة الاجتماعية لموظفي القطاع
- إستغلال الثغرات الأمنية في المواقع الإلكترونية للقطاع وتطبيقاته
- نشر البرمجيات الخبيثة عن طريق وسائط التخزين لإستخدمها من قبل موظفي القطاع
- هجمات البحث الشامل لإستغلال كلمات المرور الضعيفة لموظفي القطاع
- حجب الخدمة عن مكونات القطاع الحساسة

عصف ذهني

من وجهة نظرك
ما هي أبرز المخاطر المستقبلية في القطاع العسكري؟

أبرز المخاطر السيبرانية المستقبلية للقطاع العسكري

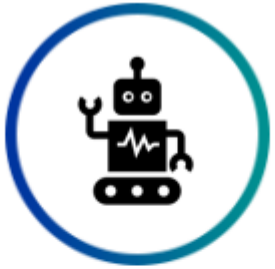
استخدام التقنية لنشر الشائعات للتأثير في الرأي العام وسمعة المؤسسات

زيادة قدرات الكيانات و الدول في إحداث تأثير سلبي على المنشآت الحساسة

نقص في المختصين بالأمن السيبراني يصل إلى 3 مليون

أبرز المخاطر السيبرانية المستقبلية للقطاع العسكري

استغلال أجهزة انترنت الأشياء للتنصت وعمل شبكات الاتصالات الخفية



استخدام تقنيات الذكاء الاصطناعي في الهجمات السيبرانية

عصف ذهني

من وجهة نظرك
ما هي المهام التنظيمية
والتشغيلية المتعلقة بالأمن
السيبراني في القطاع
العسكري؟

المهام التنظيمية للأمن السيبراني

- إعداد إستراتيجية وطنية للأمن السيبراني في القطاع والإشراف على تنفيذها
- وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني والتي تتمشى مع مستهدفات القطاع العسكري
- تحفيز وتشجيع الإبتكار والإستثمار قيما يتعلق بالأمن السيبراني للقطاع العسكري
- إجراء الدراسات والبحوث والتطوير في منهجيات الأمن السيبراني الخاصة بالقطاع العسكري
- إقتراح آليات لرفع كفاءة الإنفاق في مجالات الأمن السيبراني للقطاع العسكري
- رفع مستوى وعي موظفي القطاع العسكري
- التكامل مع تنظيمات ومستهدفات الهيئة الوطنية للأمن السيبراني

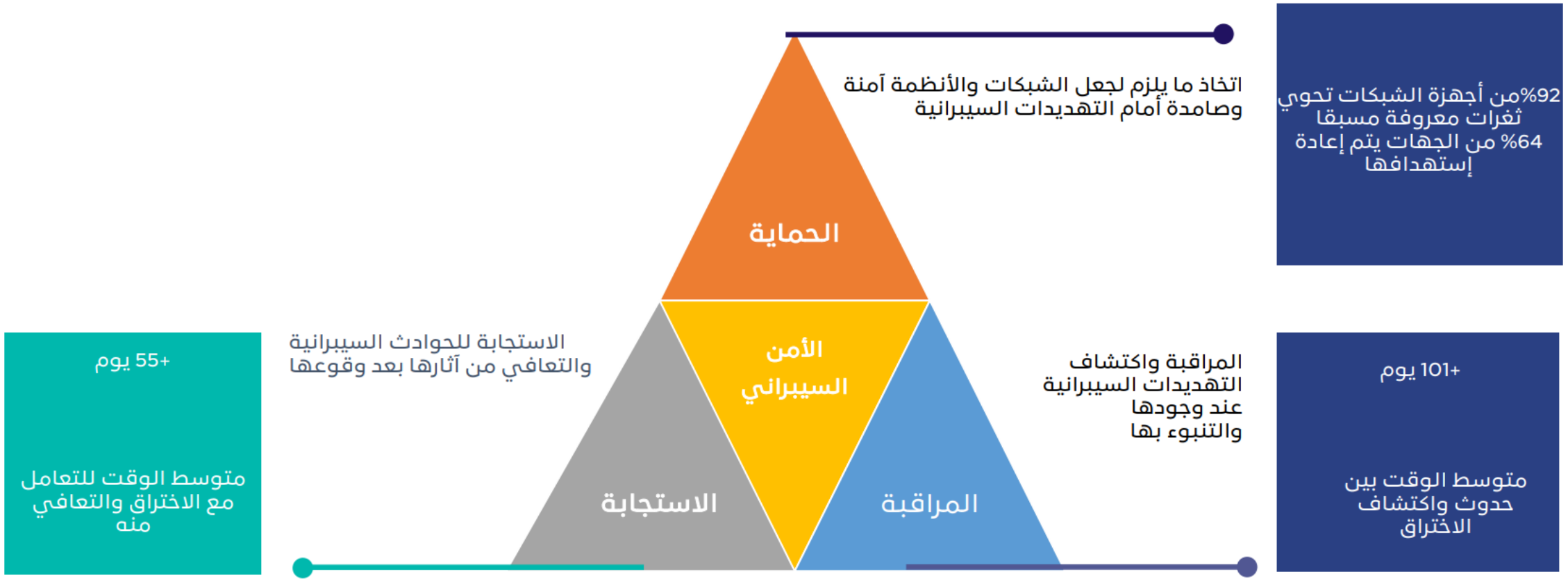
المهام التشغيلية للأمن السيبراني

- بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني بالقطاع العسكري
- إنشاء مراكز عمليات وطنية خاصة بالامن السيبراني للقطاعات العسكرية، بما في ذلك مراكز التحكم والسيطرة والإستطلاع والرصد وتبادل المعلومات الحساسة
- إشعار القطاعات العسكرية المختلفة والمعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني
- القيام بكافة بالأنشطة المتعلقة بالأمن السيبراني سواءً بنفسها أو من خلال وكلاء موثوقين

عصف ذهني

من وجهة نظرك
ما هي المنهجية المناسبة للتعامل
مع المخاطر والتهديدات
السيبرانية في قطاعك؟

منهجية المخاطروالتهديدات السيبرانية



المصدر: MandiantM-Trends 2019 Report, Source:

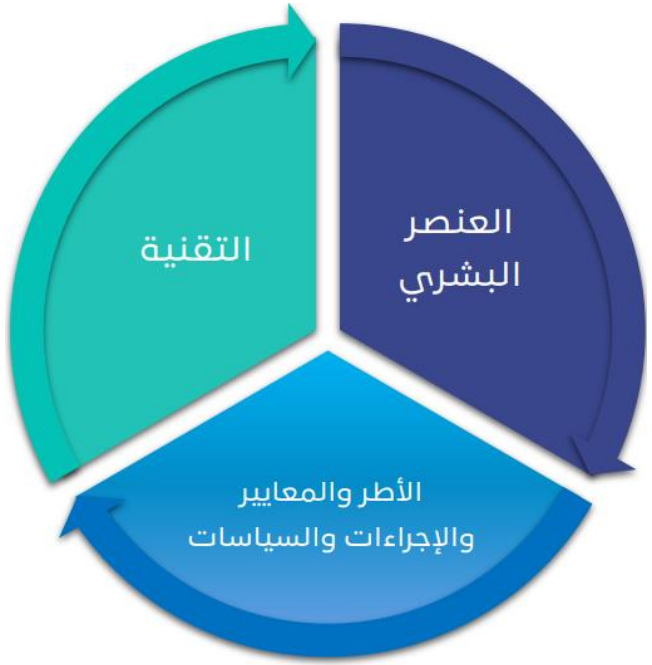
عصف ذهني

من وجهة نظرك
سبق دراسة عناصر الأمن
السيبراني، ما هي نسبة حماية
كل عنصر للفضاء السيبراني؟

عناصر الأمن السيبراني وتأثيرها في قطاعك

- تأهيل عدد كافي من المختصين (بالتعليم والتدريب)
- توعية غير المختصين

العنصر البشري تمثل 74% من الحماية



- إستخدام التقنيات المناسبة
- المراجعة المستمرة للتقنيات
- التحديثات المستمرة

التقنية تمثل 26% من الحماية

- حوكمة الأمن السيبراني
- بناء إستراتيجية للأمن السيبراني وتطبيقاتها
- تطوير سياسات وإجراءات الأمن السيبراين

العنصر البشري

العنصر البشري هو أضعف عناصر الأمن السيبراني وأكثرها خطورة

Source: Willis Towers Watson data analysis report

العنصر البشري

“المؤسسات تنفق الملايين على جدران الحماية، والتشفير، وحماية الوصول للأجهزة، وفي ذلك هدر للأموال حيث أن جيمع وسائل الحماية هذه لا تتطرق إلى الحلقة الأضعف في الأمن السيبراني وهو العنصر البشري”

كيفن ميتنك

عالم حاسوب ومستشار أمن الحاسوب (أشهر مخترقي الأنظمة)

تعزيز دور المستخدم: بعض المفاهيم الخاطئة

أمن المعلومات وحماية البيانات ليست مسؤولية متخصصي التقنية والأمن السيبراني فقط

تساهل المستخدم واعتقاده أنه لن يحدث أي اختراق من خلاله

الاعتقاد الخاطئ أن الإبلاغ عن الأنشطة المشبوهة في الفضاء السيبراني ليست مسؤولية المستخدمين وأن هناك أشخاص آخرين سوف يبلغون عنها

الاعتقاد الخاطئ أنه لن يكون هناك اختراق لجهازك بسبب عدم وجود أي معلومات سرية مخزنة لديك

مسؤولية المستخدم في الحماية من المخاطر السيبرانية

عصف ذهني

من وجهة نظرك
كيف يتم المحافظة على سرية البيانات في الفضاء السيبراني بقطاعك؟

سرية البيانات: نظام تصنيف البيانات

1.تقييم درجة الخطورة للبيانات الحساسة

عن طريق فهم لمتطلبات الخصوصية الخاصة بالمنظمة وتحديد أهداف تصنيف البيانات الخاصة بها .

2. وضع سياسة تصنيف رسمية للبيانات

الاكتفاء بتنصيف البيانات الى ٣ آو ٤ أقسام ليتم التحكم بهو تطبيقها بالشكل الصحيح

3.تعيين موقع لبياناتك

بعد تحديد أنواع البيانات ، من المهم فهرسة جميع البيانات التي يتم تخزينها إلكترونيًا.
يعتبر تدفق البيانات أحد الاعتبارات الرئيسية. كيف تقوم منظمتك بتخزين البيانات ومشاركتها داخليًا وخارجيًا؟

سرية البيانات: نظام تصنيف البيانات

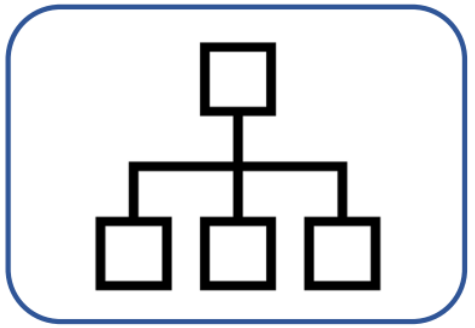
عصف ذهني

من وجهة نظرك
ما هو نظام تصنيف البيانات في قطاعك العسكري؟

أمثلة لأنظمة تصنيف البيانات

عام – Public

البيانات التي يمكن الإفصاح بشكل عام كالمواد عنها التسويقية و بيانات التواصل



داخلي - Internal

بيانات داخليه لا يمكن الإفصاح عنها خارج المنظمة كالمخططات التنظيمية للمنظمة

سري- Confidential

بيانات حساسة التي في حال اختراقها يمكن أن تؤثر بشكل سلبي على نشاط المنظمة كالعقود ومعلومات الموظفين

مقيد - Restricted

بيانات المنظمة الحساسة للغاية التي في حال تعرضت للاختراق قد تعرض المنظمة للمخاطر المالية و القانونية

Data Classification	Data Example	Security controls for Storing Accessing and Transferring
Critical/Sensitive	• Biometric data • Personal Medical Data	• Stored in encrypted format in agreed storage location e.g. SharePoint • Backed up weekly to secure local drive held in locked fireproof safe • Transferred in encrypted format • Not to be transferred by email • Accessed by Username and Password by authorised researchers only
Sensitive	• Names, addresses, dates of birth of Living individuals (Subject to GDPR)	• Stored in encrypted format in agreed storage location e.g. SharePoint • Backed up weekly to secure local drive held in locked fireproof safe • Transferred in encrypted format • Not to be transferred by email unless encrypted • Accessed by Username and Password by authorised researchers only
Internal	• Research project Communications	• Stored in in agreed storage location e.g. Email, OneDrive etc • Accessed by Username and Password • Can be transferred by email to authorised staff
Public	• Staff names, job titles and work contact details • Project Public website	• Authorised for public use on Research Project website etc • Encryption not necessary • Backed up weekly

أمثلة لأنظمة تصنيف البيانات
جامعة دبلن

أمثلة لأنظمة تصنيف البيانات
حكومة كوينزلاند

Confidentiality Requirement	Classification Label	Minimum Controls
Low	OFFICIAL	As per QGEA and agency risk assessment
Medium	SENSITIVE	As per QGEA and agency risk assessment
High	PROTECTED	As per QGEA and agency risk assessment. Agency must consider the controls outlined for PROTECTED information in ACSC ISM
National Security Information (NSI)		Not covered by QGISCF Refer to federal PSPF Seek advice from QPS

عصف ذهني

من وجهة نظرك
كيف يتم خرق سرية البيانات من
قبل موظفي قطاعك؟

كيف يتم خرق السرية؟

يمكن خرق السرية عن قصد أو غير قصد بالعديد من الطرق مثل:

- سرقة جهاز الكمبيوتر الشخصي أو القرص الصلب أو الفلاش USB
- ملفات غير مشفرة
- إرسال رسالة بريد إلكتروني إلى مستخدم غير مقصود
- مشاركة المعلومات مع مستخدم ليس لديه شرعية الوصول إليها

عصف ذهني

من وجهة نظرك
ما هي الأثار المتوقعة على قطاعك
العسكري في حال تسربت
البيانات السرية؟

تسريب البيانات السرية

01 الكشف عن معلومات المنظمة الحساسة مما يؤدي لإضرار بسمعة المنظمة أو الدولة

02 فقدان أو تلف البيانات الحساسة

03 دعاوى قضائية

04 سرقة الهوية

05 عقوبات تنظيمية

عصف ذهني

من وجهة نظرك
ما هي الإجراءات المناسبة
لحماية معرف الوصول للأنظمة
الخاص بي لكي لا يتعرض قطاعي
للمخاطر السيبرانية؟

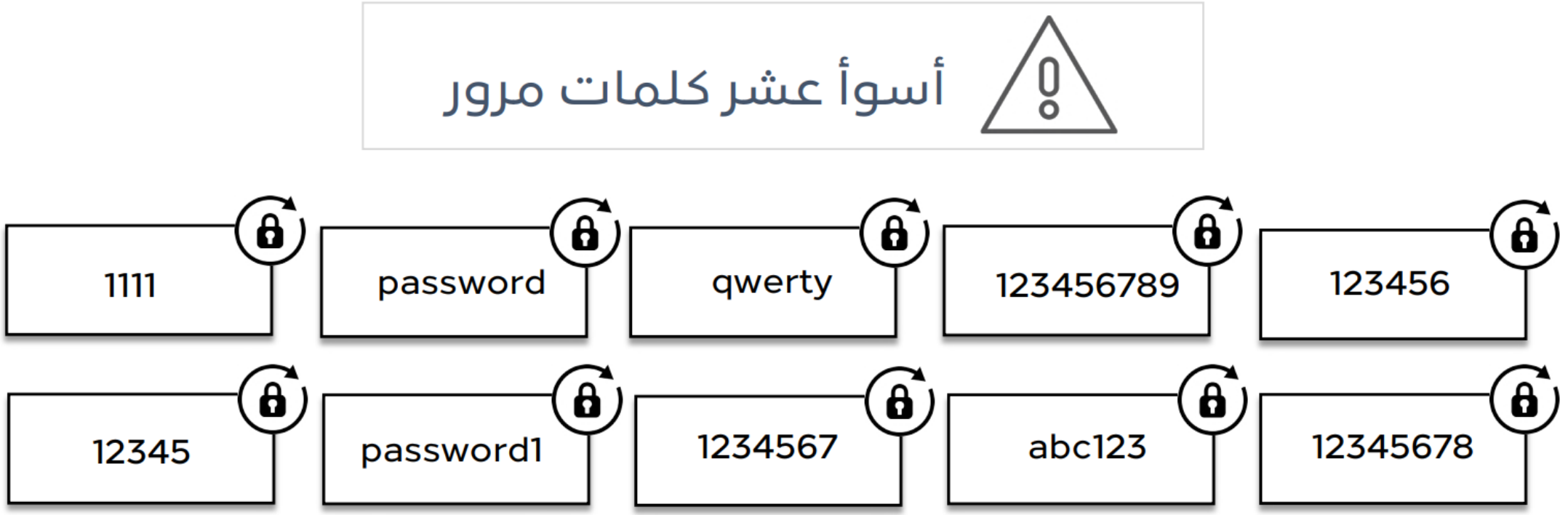
المحافظة على البيانات التعريفية الخاصة

يجب إتباع سياسة كلمة المرور الخاصة بالمنظمة التي تعمل لديها.

- قم باختيار كلمة مرور قوية
  - تستخدم 8-12 حرف على الاقل
  - تحتوي على أحرف صغيرة وكبيرة وأرقام ورموز
- تغيير كلمة المرور بشكل دوري
- تغيير كلة المرور عند الاشتباه في الإختراق أو تسربها

- **لا** تستخدم كلمة مرور تحتوي على كلمات يمكن معرفتها بسهولة
- **لا** تشارك كلمة المرور مع الآخرين
- **لا** تكتب كلمة المرور في ورقة أو تحفظها في ملف
- **لا** تستخدم رقم الهوية أو رقم الجوال أو تاريخ الميلاد أو أي بيانات شخصية في كلمة المرور
- **لا** تستخدم نفس كلمة المرور لحسابات مختلفة

المحافظة على البيانات التعريفية الخاصة



عصف ذهني

من وجهة نظرك
كم من الوقت يستغرقه المهاجم
للحصول على كلمة المرور؟

المدة التي يحتاجها المهاجك لكسر كلمة
المرور تعتمد على مدى صعوبتها

بعض سياسات الأمن السيبراني: الإستخدام العادل

- يجب إستخدام موارد المؤسسة للأغراض المصرح بها فقط
- أنت مسؤول عن جميع الأنشطة على معرف المستخدم الخاص بك أو التي تنشأ من نظامك
- يجب إستخدام الإصدارات الأصلية فقط من البرامج
- الوصول فقط إلى المعلومات الخاصة بك، أو المعلومات العامة، أو التي تم منحك تصريح للوصول لها
- يجب عليك قفل الشاشة أو تسجيل الخروج عند ترك الجهاز
- عدم إستخدام مواقع التواصل الاجتماعي للإضرار بالمؤسسة أو أحد الموظفين

عصف ذهني

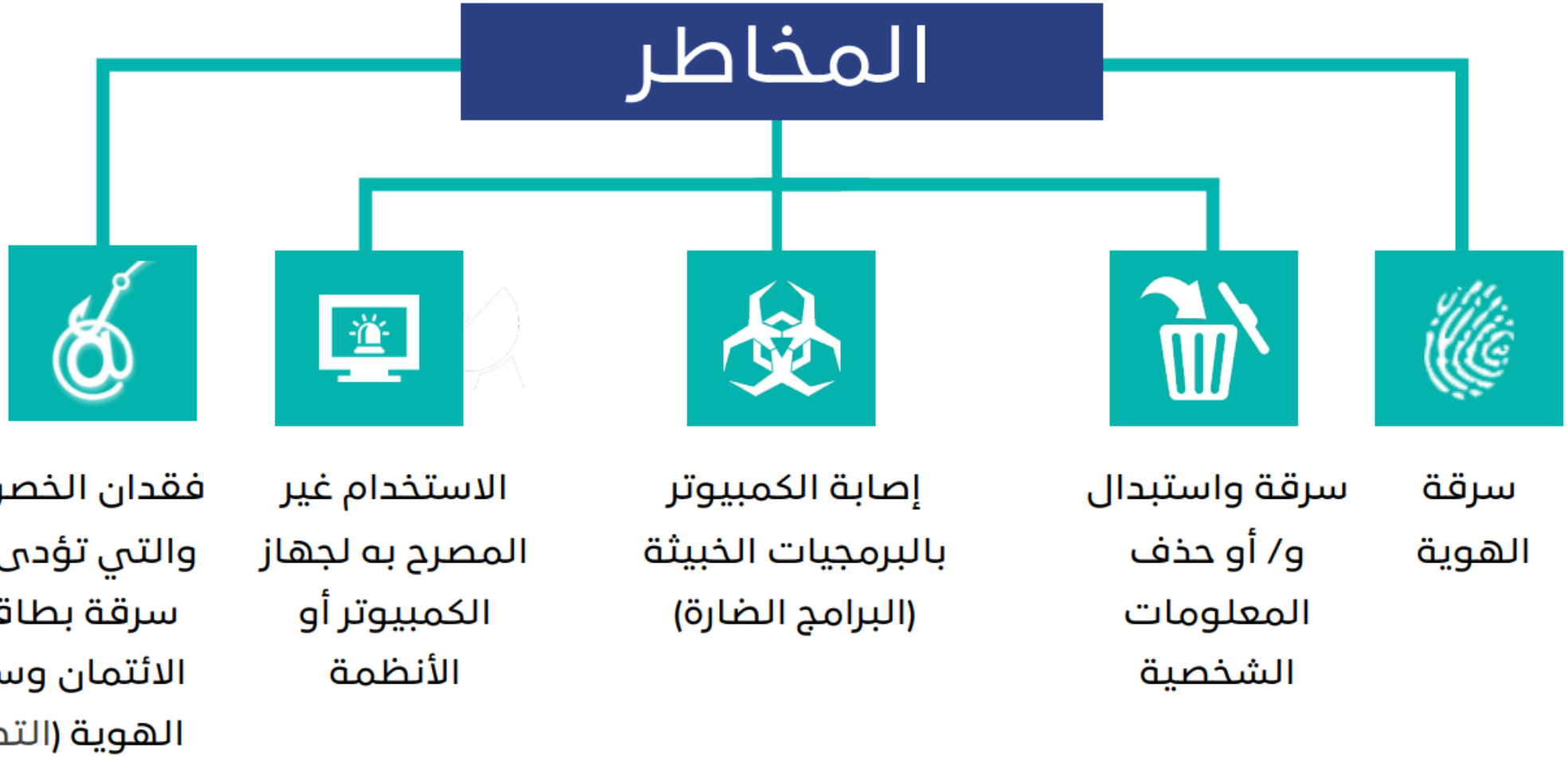
من وجهة نظرك
هل للوثائق الورقية دورفي فضاءنا السيبراني؟

- يجب الإقفال على الوثائق الحساسة عند ترك المكتب لفترة طويلة
- إزالة جميع الوثائق من المكتب ووضعها في الخزائن أو الأدراج محكمة الإغلاق

عصف ذهني

من وجهة نظرك
هل التصفح من خلال أجهزة
قطاعك الوظيفي معرضه
للمخاطر؟ أذكر أمثلة عليها؟

المخاطر المتعلقة بمتصفحات الويب



عصف ذهني

من وجهة نظرك
ما المقصود بمفهوم المو اقع
الخبيثة؟

ماهي المواقع الخبيثة ؟

هي المواقع الإلكترونية التي تزعم تثبيت برامج قد تضر بجهازك إما عن طريق تعطيل جهاز الكمبيوتر او جمع المعلومات الشخصية من الجهاز أو التحكم الكامل بجهازك .

كيف أحمي جهازي منها ؟

استخدم برنامج مكافحة فيروسات محدث وموثوق لحماية جهازك.

زيارة المواقع الموثوقة فقط وتأكد من أنها مشروعة.

أترك الموقع على الفور إذا بدت عليه الشبهات وحاول تنفيذ أمر معين من خلال متصفحك.

موقع التصيّد

موقع وهمي صمم للحصول على اسم المستخدم و كلمة المرور الخاصة به.

عصف ذهني

من وجهة نظرك
ما هي أفضل الممارسات عند
استخدام متصفح الويب
في قطاعك؟

أفضل ممارسات إستخدام متصفح الويب

استخدم متصفح انترنت آمن

استخدم النسخة الأحدث من المتصفح وحدثه بإنتظام.

قم بتحديث نظام التشغيل و التطبيقات التي تعمل مع المتصفح مثل تطبيقات الوسائط المتعددة

استخدم أحد برامج مكافحة الفيروسات وبرامج مكافحة التجسس المحدثة.

استخدم برنامج جدار حماية محدث.

قم بمسح ملفات تعريف الارتباط للمواقع

البريد الإلكتروني

- التكنولوجيا الأكثر شيوعا لهجمات الهندسة الاجتماعية.
- الجميع يستخدم البريد الإلكتروني.
- أصبح وسيلة رسمية في المخاطبات.
- يستخدم المجرمون أجهزة كمبيوتر مخترقة لإرسال الملايين من رسائل البريد الإلكتروني كل يوم (البريد المزعج).

293 مليار رسالة ترسل يومياً

45% رسائل دعائية

عصف ذهني

من وجهة نظرك
ما هي تهديدات ومخاطر البريد
الإلكتروني المحتمله؟

تهديدات ومخاطر البريد الإلكتروني

التصيّد

الهندسة الإجتماعية

المرفقات الخبيثة (الضارة)

البريد المزعج

الروابط الخبيثة

قرصنة البريد الإلكتروني

التصيد بالبريد الإلكتروني

هو نوع من أنواع الاحتيال باستخدام البريد الإلكتروني حيث يرسل المحتال بريد إلكتروني شرعي ظاهريا ويبدو ككيان موثوق به ولكنه مصمم لاستخراج المعلومات الحساسة.

هل تعلم؟

أن رسائل التصيّد الإلكترونية الإحتيالية تشكل 47% من هجمات الهندسة الإجتماعية التي تستهدف الشركات.

التصيد بالبريد الإلكتروني: مثال

- تأكد من عنوان الرسالة والبريد المرسل
- تأكد من لغة البريد الإلكتروني (أخطاء إملائية)
- وضع بعض النقاط الحقيقة للتضليل
- في بعض الحالات، وجود عبارات تهديد
- لا تقم بفتح الروابط أو المرفقات
- لا تقم بالرد على البريد الإلكتروني

عصف ذهني

من وجهة نظرك
ما هي الإجراءات المتبعه لحماية البريد الإلكتروني الوظيفي؟

حماية البريد الإلكتروني

تأكد من معلومات الشخص المرسل (الاسم و البريد الإلكتروني)

لا تقم بالرد على رسائل البريد الإلكتروني غير المرغوب فيها والتي تطلب ملء نموذج أو تقديم معلومات شخصية أو مالية على الرابط المضمن.

قبل فتح الملفات الملحقة قم بفحصها باستخدام برامج مكافحة الفيروسات

لا تفتح الملحقات او الروابط في الرسائل غير المرغوب فيها

عصف ذهني

من وجهة نظرك
ما هي تهديدات ومخاطر جهازك
الشخصي في المقر الوظيفي؟

البرمجيات الخبيثة والضارة

01

فيروسات

الفيروس هو برنامج مصمم خصيصا للإضرار أو نسخ البيانات من جهاز الكمبيوتر الخاص بك.

02

أحصنة طروادة

حصان طروادة هو برنامج يبدو مشروعا ولكنه في الواقع برنامج خبيث يضر البيانات في الكمبيوتر ويسرق المعلومات الحساسة.

03

برامج التجسس

برنامج يتجسس على جهاز الكمبيوتر الخاص بك ويتتبع أنشطتك الخاصة.

الهدف من البرمجيات الخبيثة والضارة

كيفية إنتشار البرامج الخبيثة

1. وسائل التخزين القابلة للإزالة : USBs و CDs
2. مرفقات البريد الالكتروني
3. مواقع الويب التي تحتوي على البرامج الخبيثة
4. ضمن بعض البرامج أو التطبيقات
5. تبادل الملفات
6. البرامج التي تم قرصنتها
7. مواقع التواصل الاجتماعي

عصف ذهني

من وجهة نظرك
كيف أحمي جهازي الوظيفي؟

كيف تحمي جهازك الوظيفي من التهديدات:

يمكنك حماية الكمبيوتر الشخصي بإستخدام الأساليب التالية:

عصف ذهني

من وجهة نظرك
هل من المعقول أن هاتفك المحمول له أثرعلى أنظمة قطاعك؟ كيف؟

من تهديدات الهواتف المحمولة

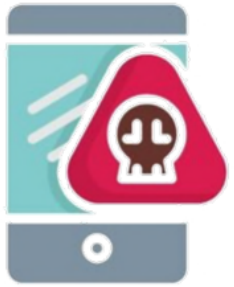
01 تحميل تطبيقات الهاتف الضارة و التجسسية

02 خرق الخصوصية وتحديد الموقع

03 فقدان البيانات بسبب سرقة أو فقدان الهاتف المحمول أو مسح أو حذف الملفات بداخله

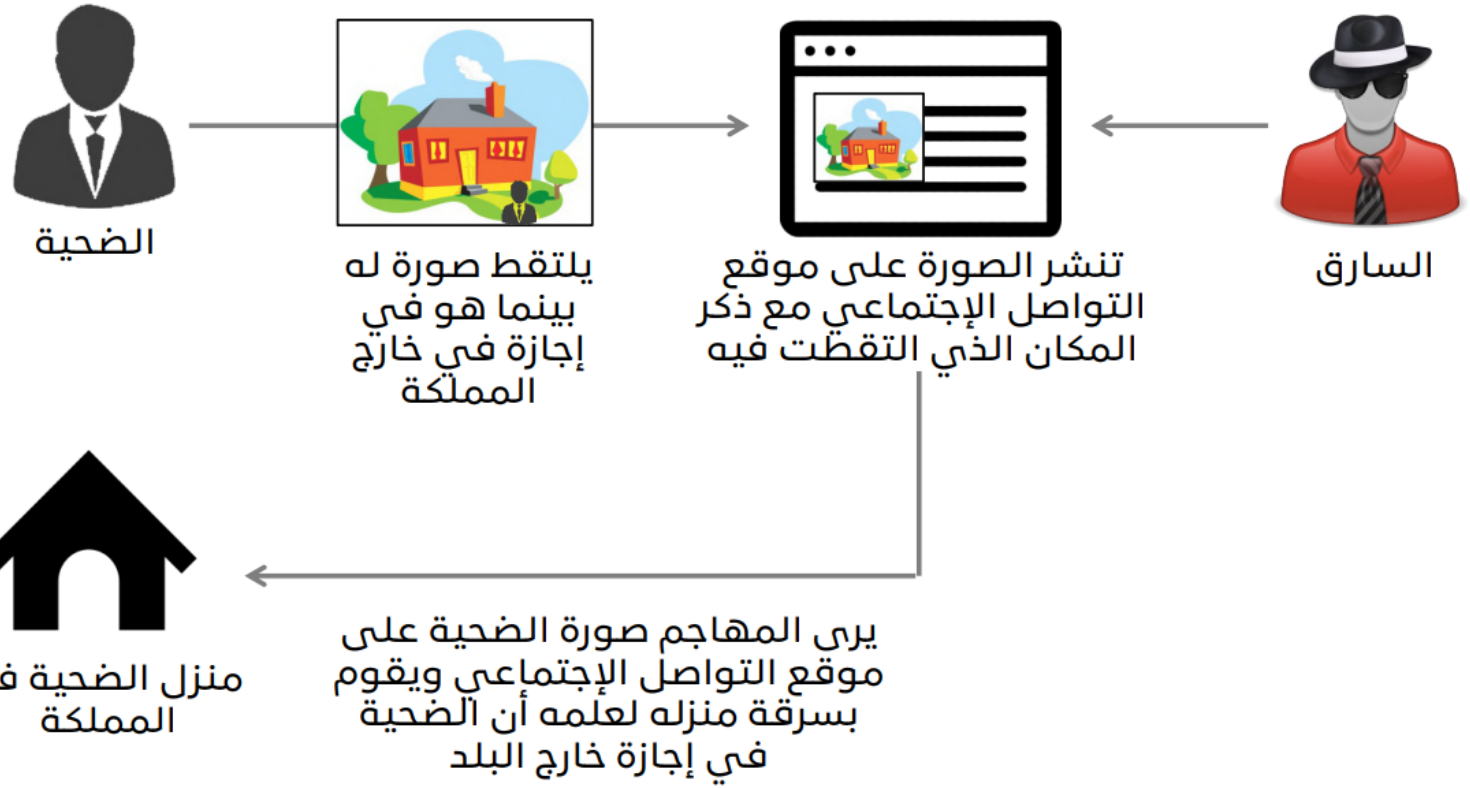
04 الهندسة الاجتماعية عن طريق الرسائل القصيرة (SMS)

05 استخدام شبكة واي فاي عامة او بلوتوث غير محمية

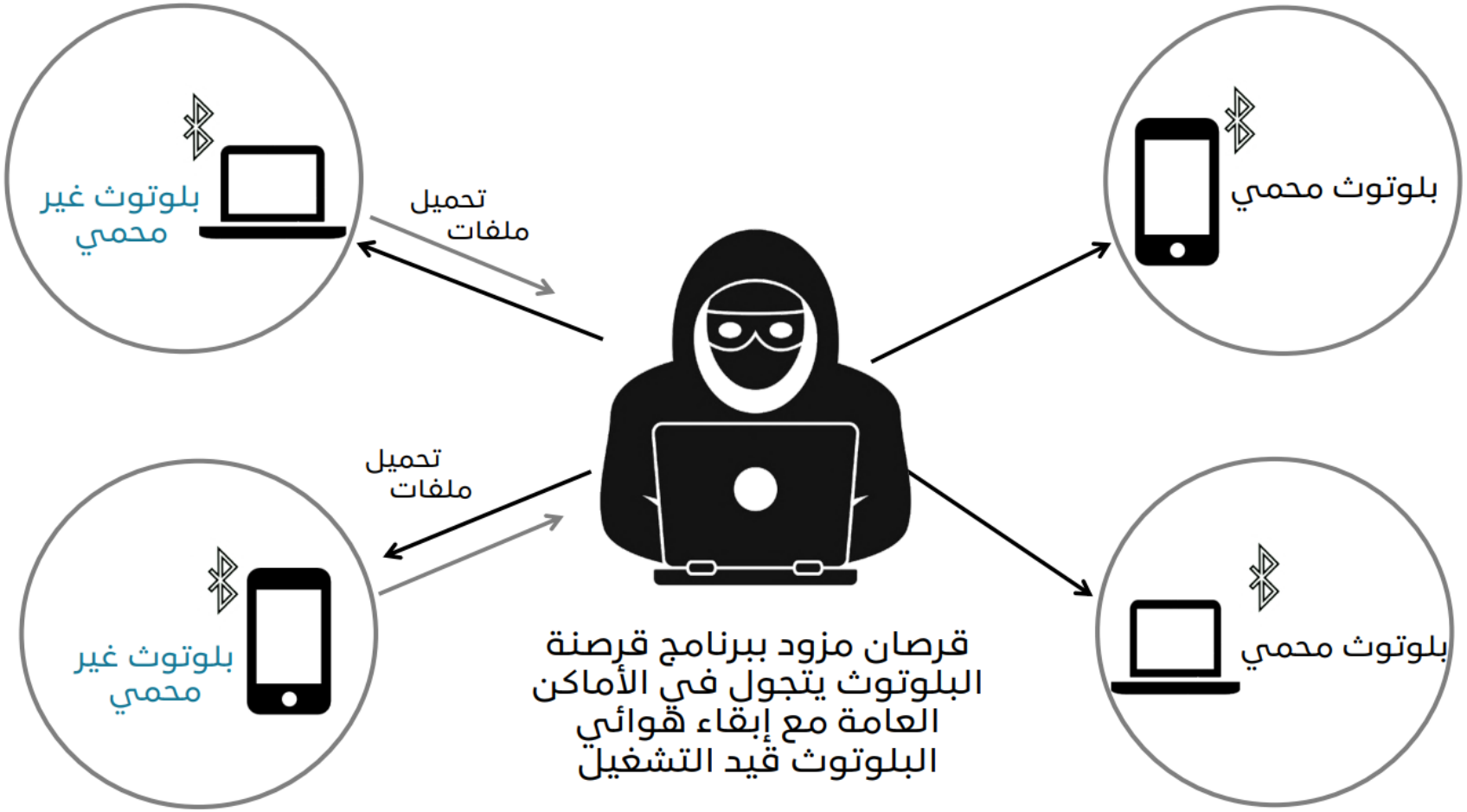


تطبيقات التجسس (الضارة)

تهديد تحديد الموقع الجغرافي



قرصنة البلوتوث



البلوتوث والواي-فاي

قد يتم اعتراض المعلومات الحساسة المرسلة عن طريق البلوتوث أو الواي-فاي.

من السهل إستغلال وظائف البلوتوث أو الواي-فاي لإرسال برمجيات ضارة.

قم بتعطيل كلا من البلوتوث والواي-فاي عندما لا تكون هناك حاجة لهم.

يتيح البلوتوث لهاتفك الإتصال لاسلكيا مع الأجهزة الأخرى مثل سماعات الرأس والهواتف المحمولة الأخرى أو مع الكمبيوتر.

عصف ذهني

مما سبق ذكره
ما هي الممارسات الآمنة
للموظفين التي يجب أخذها
بعين الإعتبار؟

الممارسات الآمنة للموظفين

١. اتباع الاحترازات والإجراءات الأمنية في المرافق:
٢. الالتزام بالسياسات والضوابط الأمنية:
٣. حماية بيانات حساب المستخدم وكلمات المرور:
٤. الاستخدام الآمن للإنترنت ووسائل التواصل الاجتماعي:
٥. الحذر من حملات التصيّد الإلكتروني والهندسة الاجتماعية:
٦. حماية البريد الإلكتروني:
٧. تحميل البرامج والأدوات الأصلية وتحديث الأنظمة:
٨. تصنيف ومشاركة الملفات:

الممارسات الآمنة للموظفين

٩. النسخ الاحتياطي للبيانات ونقلها من مكان لآخر:

١٠.استخدام الخدمات السحابية:

١١. برامج الاجتماعات الافتراضية والعمل عن بُعد:

١٢. أجهزة العمل أثناء التنقل والسفر:

١٣. أمن الأجهزة الشخصية المتنقلة:

١٤. الاستخدام الآمن للطابعات اللاسلكية وأجهزة إنترنت الأشياء (IoT[٩]):

١٥. مغادرة المكتب:

١٦. مراقبة علامات حدوث الخطر السيبراني:

١٧. الإبلاغ عن الاختراقات والأحداث المريبة:

شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -