

مساق قضايا إعلامية

د. منى المصري

DGM 335

المحاضرة الرابعة



الأمن والسلامة الرقمية للإعلاميين والمسوقين

المحاضرة الرابعة

مدرس المساق:
د. منى المصري

محاور المحاضرة

- ✓ الأمن والسلامة الرقمية كضرورة مهنية في الإعلام والتسويق
- ✓ المخاطر السيبرانية وحماية البيانات وأساليب الوقاية منها
- ✓ استراتيجيات السلامة الرقمية المهنية والأدوات المساندة
- ✓ البصمة الرقمية والهوية المهنية وبناء السمعة الرقمية الآمنة
- ✓ الأطر القانونية والأخلاقية للأمن الرقمي وحماية الخصوصية
- ✓ التطبيق العملي: إعداد خطة سلامة رقمية متكاملة لفريق إعلامي أو تسويقي

أهداف المحاضرة

بنهاية هذه المحاضرة، ستكون قادرًا على:

- ✓ تفسير مفهوم الأمن والسلامة الرقمية وأهميته في العمل الإعلامي والتسويقي الحديث
- ✓ تمييز أنواع المخاطر السيبرانية التي تواجه الصحفيين والمسوقين، وتحليل تأثيرها على المؤسسات والأفراد
- ✓ تطبيق استراتيجيات عملية للحماية الرقمية تشمل إدارة البيانات، تأمين الحسابات، ومواجهة الهجمات الإلكترونية
- ✓ تحليل العلاقة بين البصمة الرقمية والهوية المهنية وتقييم أثرها على السمعة الرقمية للأفراد والمؤسسات
- ✓ بناء خطة متكاملة للأمن الرقمية المهنية تتضمن إجراءات وقائية وتدريبية وإدارية
- ✓ تقييم الجوانب القانونية والأخلاقية المرتبطة باستخدام البيانات الرقمية وحماية الخصوصية

مقدمة

يشهد العالم اليوم تصاعداً غير مسبوق في حجم الهجمات السيبرانية التي تستهدف الأفراد والمؤسسات، وبصورة خاصة العاملين في مجالات الإعلام والتسويق الرقمي. فهؤلاء المهنيون يعتمدون على الإنترنت ومنصات التواصل الاجتماعي كأدوات عمل رئيسية، ويتعاملون يومياً مع بيانات حساسة: مصادر، شرائح جمهور، خطط حملات، محتوى مُنتج، ومرجعيات قانونية. أي اختراق أو تسريب يؤثر مباشرة على المصداقية المهنية، العلاقة مع المصادر، وسمعة العلامة التجارية.

إن الأمن الرقمي إذاً ليس ترفاً تقنياً بل عنصر جوهري لممارسة مهنية أخلاقية ومستدامة. مثال: فقدان حساب رسمي لشركة يؤدي لإرسال محتوى مضلل للجمهور وإضرار العلامة التجارية. تتناول هذه المحاضرة الأسس النظرية والعملية للأمن والسلامة الرقمية، وتقدم أدوات عملية للإعلاميين والمسوقين لحماية بياناتهم المهنية والشخصية، وبناء سمعة رقمية مستقرة وأمنة على المدى الطويل.

تعريف الأمن السيبراني

الأمن السيبراني هو مجموعة الممارسات والتقنيات المصممة لحماية الأنظمة، والشبكات، والبرامج، والبيانات من الهجمات الرقمية التي تهدف إلى الوصول غير المصرح به أو إتلاف المعلومات أو تعطيل العمليات. يُعد أحد أهم مكونات الأمن الوطني والمؤسسي في العصر الرقمي.

أبرز أنواع المخاطر السيبرانية:

- **البرمجيات الخبيثة:** (Malware): برامج تُزرع في الأجهزة بهدف سرقة المعلومات أو التجسس
- **التصيد الإلكتروني:** (Phishing) رسائل أو روابط مزيفة تُستخدم لخداع المستخدمين والحصول على بياناتهم
- **الاختراق:** Hacking الدخول غير المشروع إلى حسابات أو أنظمة إلكترونية
- **تسريب البيانات:** (Data Breach): الكشف غير المقصود أو المتعمد لمعلومات حساسة
- **الهندسة الاجتماعية:** (Social Engineering) التلاعب النفسي بالمستخدمين لإقناعهم بالإفصاح عن معلومات

البصمة الرقمية

DIGITAL FOOTPRINTS

What do yours say?

BE CAREFUL ABOUT:

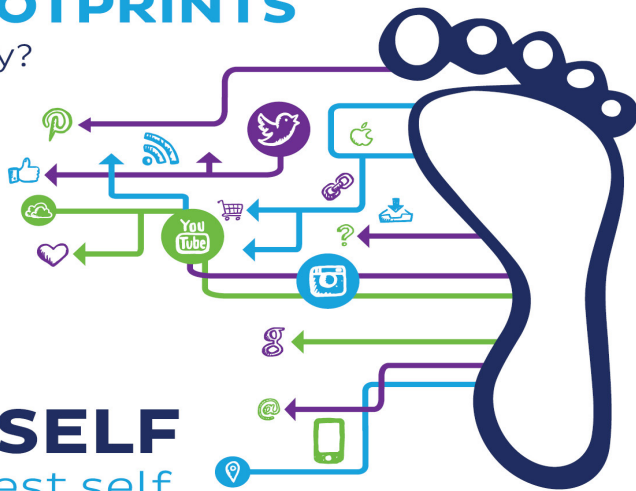
- What you share.
- Where you share.
- With whom you share.

BE SMART ABOUT:

- Sites you visit.
- Emails you open.
- Links you click.

BE YOURSELF

but be your best self.



البصمة الرقمية (Digital Footprint) تُعرّف أكاديمياً بأنها مجموعة السجلات والآثار الرقمية المتولدة عن نشاط فرد أو مؤسسة عبر الإنترنت، بما في ذلك المشاركات، التعليقات، عمليات البحث، سجلات التصفح، وبيانات التعريف. البصمة قد تكون سلبية أو إيجابية وتؤثر على إمكانية تتبع المعلومات وصياغة التقييمات الآلية عن الأفراد أو المنظمات.

مثال : بحث سريع عن اسم صحفي يظهر مقالات قديمة، صور، وتغريدات تعكس مواقف سابقة.

DIGITAL
FOOTPRINT

الأمن والسلامة الرقمية كضرورة مهنية

حادثة اختراق وكالة "أسوشيتد برس" كمثال على المخاطر السيبرانية في المجال الإعلامي: Associated Press - AP وهي واحدة من أقدم وأكبر وكالات الأنباء في العالم، تأسست عام 1846 ومقرها في نيويورك، وتعد مصدرًا رئيسيًا للأخبار لآلاف المؤسسات الإعلامية حول العالم. في عام 2013، تعرّض حساب وكالة "أسوشيتد برس" (Associated Press - AP) على منصة "تويتر" للاختراق، ونُشرت تغريدة زائفة جاء فيها:

"انفجاران في البيت الأبيض وإصابة الرئيس أوباما."

أدت هذه التغريدة إلى انخفاض فوري في مؤشر "داو جونز" الصناعي الأمريكي بأكثر من 140 نقطة خلال دقائق، قبل أن تؤكد الوكالة لاحقًا أن الحساب تم اختراقه. تُعد هذه الحادثة نموذجًا عمليًا يوضح مدى خطورة الهجمات السيبرانية على المؤسسات الإعلامية وتأثيرها المباشر على الأسواق، والرأي العام، والموثوقية المهنية.

<https://apnews.com/general-news-68a43f18c9aa4a87bfbf350a566404c9?>

عقب انتشارها، تم تعليق حساب AP على تويتر مؤقتًا، وأكدت الوكالة لاحقًا أن التغريدة كانت نتيجة اختراق، وأوضحت أن الأمر بدأ بمحاولة تصيد (Phishing) تستهدف الشبكة الداخلية للوكالة. أثر الهجوم كان سريعًا وخطيرًا: الأسواق اضطربت، الأخبار انتشرت، والتصحيح جاء بعد دقائق فقط عندما أوضحت AP أن التغريدة كانت خاطئة.

الأمن والسلامة الرقمية كضرورة مهنية

الأمن الرقمي لم يعد مجالًا تقنيًا بحتًا، بل أصبح جزءًا من الثقافة المهنية لأي صحفي أو مسوّق. فكل محتوى يُنتج أو يُنشر أو يُشارك على الإنترنت هو جزء من منظومة بيانات مترابطة، يسهل تتبعها واستغلالها.

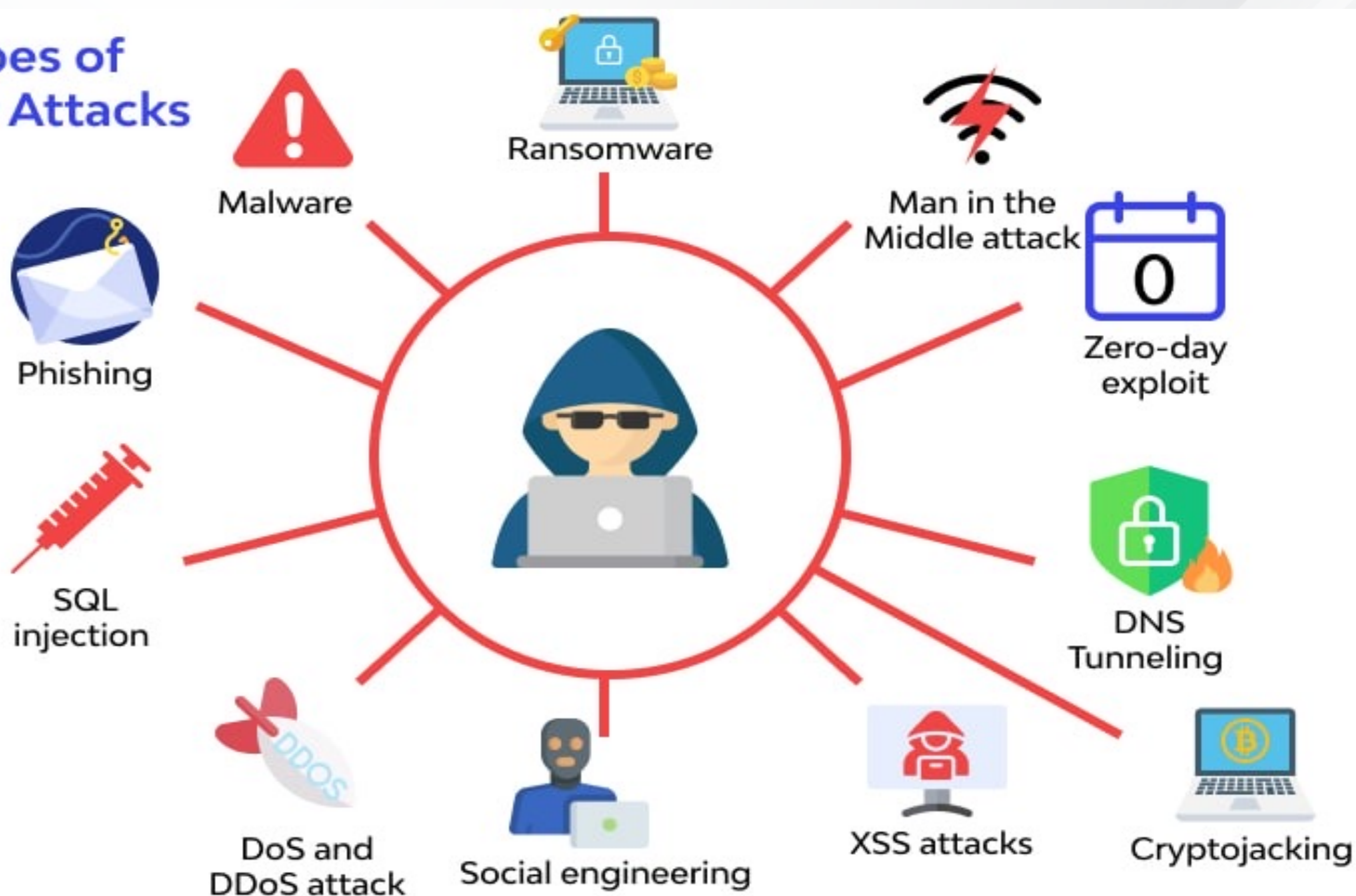
مفاهيم أساسية:

الأمن الرقمي (Digital Security) حماية المعلومات والأجهزة والأنظمة من الوصول غير المصرّح به أو التلاعب.

السلامة الرقمية (Digital Safety) تشمل الأبعاد التقنية والنفسية والاجتماعية لحماية المستخدم من الأذى أثناء النشاط الرقمي.

للمناقش: كيف يمكن لمؤسسة إعلامية أن توازن بين حرية النشر والحفاظ على أمن بياناتها الداخلية؟

Types of Cyber Attacks



التصيد الاحتيالي

التصيد (Phishing) هو هجوم يحاكي جهات موثوقة لخداع الضحية للكشف عن بيانات حساسة أو لزرع برمجيات.

علامات التصيد:

1. عنوان مرسل غير متطابق
2. روابط مختصرة تقود لمواقع مزيفة
3. أخطاء لغوية أو استعجال غير مبرر

مثال : رسالة تفيد بضرورة "تحديث" كلمة المرور عبر رابط؛ الحل: المرور عبر الموقع الرسمي والتحقق من شهادة الأمان.



Let's Go Phishing!

البرمجيات الخبيثة والـRansomware



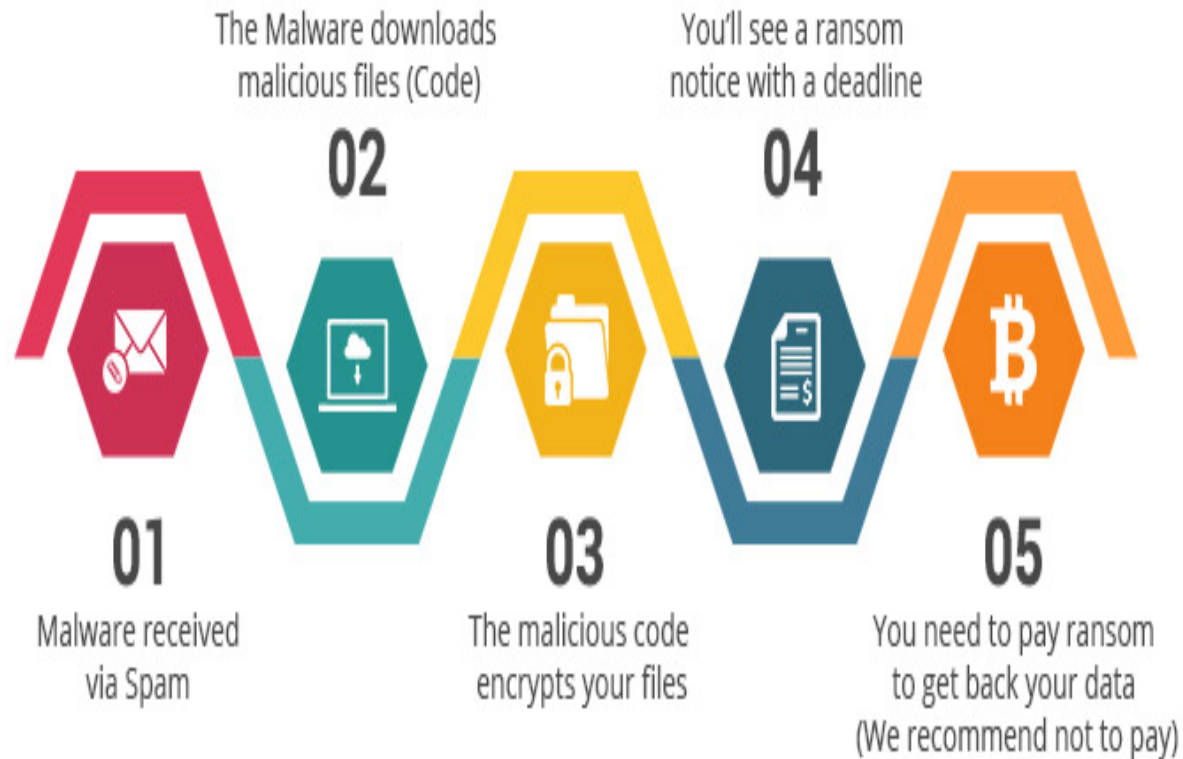
Ransomware Attacks

البرمجيات الخبيثة تشمل فيروسات، وبرمجيات فدية تُشفّر الملفات وتطالب بفدية لاستعادتها. الاعتماد على نسخ احتياطية منفصلة وتحديث أنظمة التشغيل يساهمان في التخفيف من الضرر.

الخطوة الأولى عند الإصابة: عزل الجهاز عن الشبكة وإخطار فريق تقنية المعلومات.

البرمجيات الخبيثة والـ Ransomware

How Ransomware Works



How Social Engineering Works



الهندسة الاجتماعية والتهديدات غير التقنية

Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.



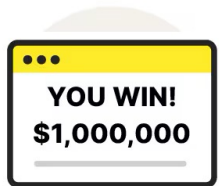
Your 'friend' sends you a strange message.



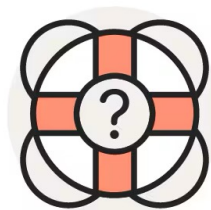
Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You're receiving help you didn't ask for.



The sender can't prove their identity.

الهندسة الاجتماعية تستخدم الإقناع والاستغلال النفسي لخداع موظفي المؤسسات لكشف معلومات أو منح صلاحيات.

أساليب شائعة:

1. انتحال صفة موظف داخلي

2. ضغط زمني

3. طلب الوصول لطوابع أو ملفات

الوقاية تشمل التدريب الدوري، قواعد توثيق الهوية قبل مشاركة المعلومات، وسياسات "لا مشاركة كلمات المرور".

مثال: مكالمة تبدو من مزود خدمة تطلب تأكيد بيانات حساسة.

امثلة على استخدام أسلوب الهندسة الاجتماعية والروابط الوهمية



Coronaraby

Mar 28 at 13:15 • 🌐

مستقبلنا بأيديكم ... أهمية البقاء بالمنزل بالارقام

<https://www.coronaaraby.com/predict>



CORONARABY.COM

إوعدنا تفحص

تأكد من عدم إصابتك بفيروس كورونا من خلال ا...

LEARN MORE

19

1 Comment



Like



Comment



Share



مريم العراق



@SA9Fjj2UPxdnEgp · متابعة

اطلقت مفوضية الامم المتحدة للاغاثة حملة تقدم مساعدات لفائدة المتضررين من جائحة covid-19

يمكن لأي شخص الاستفادة من المساعدة المالية عبارة عن 800 دولار شهريا لمدة 4 اشهر

تحقق ما اذا كنت مؤهلا

getmenows.blogspot.com/?covid19



١٠:٤٠ ص ١٠٠ أكتوبر ٢٠٢١

الاطلاع على أحدث المعلومات حول فيروس ك...



قراءة المزيد على X

الهندسة الاجتماعية والتهديدات غير التقنية

يظهر هذا المقال حجم الخطر والهجمات السيبرانية التي تعرضت لها العديد من الشركات والمؤسسات العربية في آخر ٣ سنوات. ويوضح مصادرها وأسبابها وأهم المشكلات الناجمة عنها

<https://www.alborsaaneews.com/2024/09/22/1827902>

70% من الشركات العربية تعرضت لهجمات "سيبرانية" خلال السنوات الثلاث الماضية

كتب : محمد فوزي — الأحد 22 سبتمبر 2024



المخاطر على الإعلاميين والمسوقين

Types of CYBER ATTACKS



Phishing and
Social Engineering



Ransomware
Attacks



Insider Threats



Internet of Things
(IoT) Vulnerabilities



Cloud Security
Challenges

• سرقة الحسابات أو البريد الإلكتروني المهني

• تسريب المعلومات الصحفية أو الخطط التسويقية قبل نشرها

• استخدام الهوية الرقمية في حملات تضليل أو نشر أخبار مزيفة

• تشويه السمعة المهنية أو الشخصية عبر فبركة المحتوى

أسباب تعرض الإعلاميين والمسوقين للمخاطر الرقمية

العاملون في الإعلام والتسويق يُستهدفون لعدة أسباب:

1. وصولهم لمعلومات حساسة
 2. تفاعلهم مع جماهير واسعة
 3. إدارتهم لعدة حسابات مرتبطة بمصادر ومعلنين
 4. بيئة الضغط الزمني تزيد من الأخطاء البشرية
- لذا التوعية والسلوك المهني أمران أساسيان للوقاية من هذه التهديدات.

مثال: مسؤول وسائل تواصل يشارك رابطاً دون مراجعة يؤدي لانتشار خبر

خاطئ.



أساليب حماية البيانات في المؤسسات الإعلامية

1. تفعيل المصادقة الثنائية (Two-Factor Authentication) لجميع الحسابات

2. تخزين البيانات الحساسة على خوادم آمنة ومشفرة

3. تدريب فرق العمل على التعرف إلى محاولات الاختراق

4. وضع سياسات خصوصية داخلية تنظم الوصول إلى البيانات



أساليب الوقاية الأساسية

• إدارة كلمات المرور

- ✓ استخدم كلمات مرور طويلة وفريدة لكل حساب
- ✓ استخدم مدير كلمات مرور موثوق
- ✓ فعل المصادقة متعددة العوامل (MFA) لكل حساب مهني
- ✓ تجنب مشاركة كلمات المرور عبر البريد أو الرسائل النصية

• التشفير — أساسيات وتطبيقات عملية

التشفير يحول البيانات لصور غير مفهومة ما لم يتوفر مفتاح فك التشفير. يجب تشفير الرسائل الحساسة، الملفات، والنسخ الاحتياطية أثناء النقل والتخزين. أدوات التشفير البريدية وبرامج التخزين السحابي الآمنة ضرورية للتعامل مع المصادر الحساسة.

مثال: استخدام PGP أو ميزة التشفير في خدمات البريد لتأمين المراسلات مع مصدر حساس.

أساليب الوقاية الأساسية

• النسخ الاحتياطية واستراتيجيات التعافي

استعمل قاعدة 1-2-3 للنسخ الاحتياطية: ثلاث نسخ من البيانات، على الأقل في وسيطين مختلفين، ونسخة واحدة خارج الموقع أو غير متصلة بالإنترنت. اختبر استعادة النسخ بانتظام للتأكد من صلاحيتها. النسخ الاحتياطية المشفرة تحمي من طلبات الفدية.

• فصل الحسابات والحد من الصلاحيات

افصل الحسابات الشخصية عن المهنية، وطبق مبدأ "الأقل صلاحية" Least Privilege لمنح الوصول الضروري فقط. استخدم حسابات خدمة منفصلة للأنظمة الآلية وكلمات مرور منفصلة للمسؤولين. هذا يقلل من نطاق الضرر عند اختراق حساب واحد.

مثال: حساب منشورات فريق التواصل الاجتماعي مستقل عن حسابات المدفوعات الإعلانية.

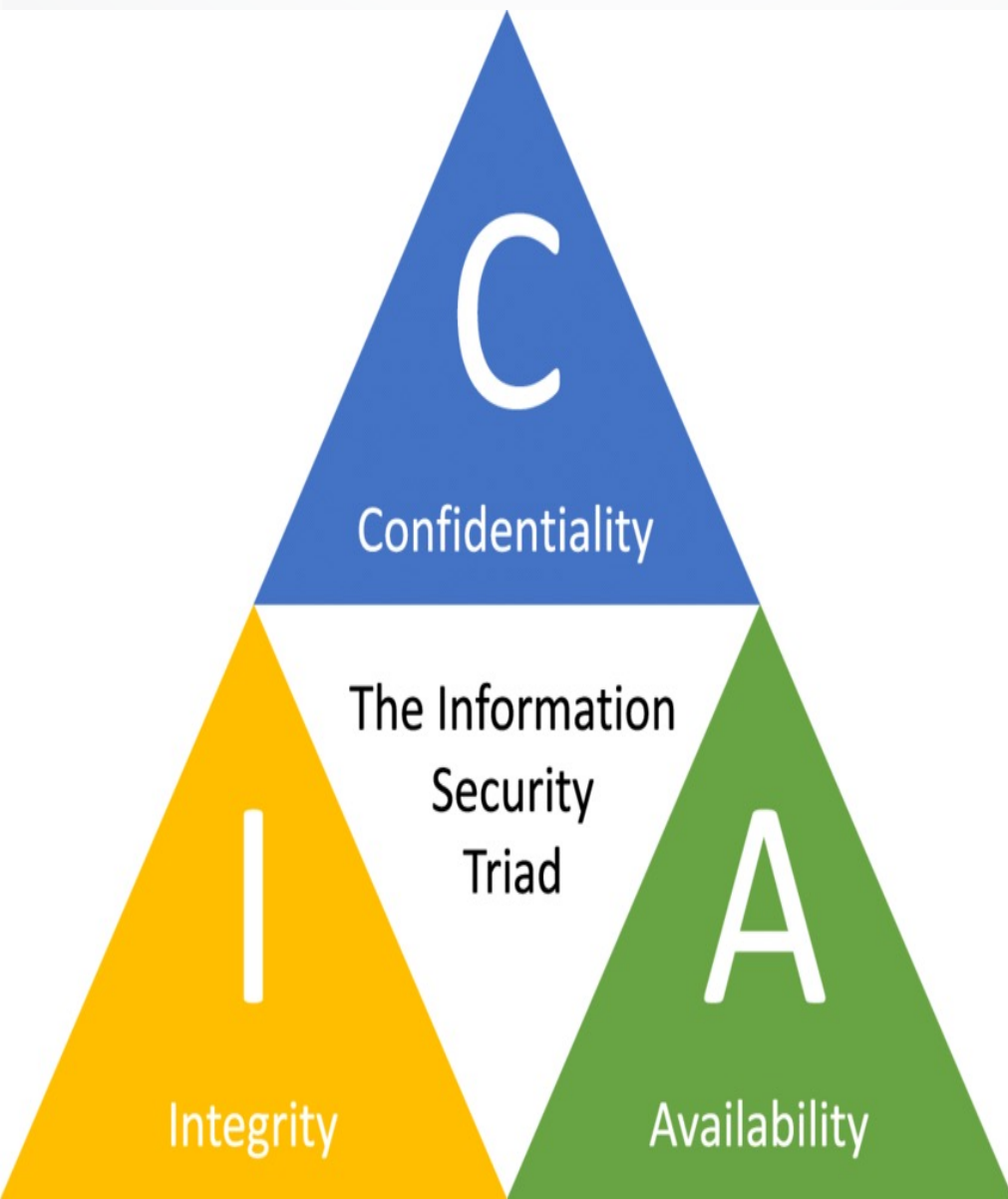
استراتيجيات السلامة الرقمية المهنية

تشير السلامة الرقمية المهنية إلى مجموعة الممارسات والسلوكيات التي تحافظ على أمن المهنيين أثناء استخدامهم للمنصات الرقمية. تتعلق هذه الاستراتيجيات ليس فقط بالحماية التقنية، بل أيضاً بالوعي الشخصي والمسؤولية الأخلاقية.

مبادئ السلامة الرقمية:

- الوعي بالمخاطر المحتملة في كل تفاعل رقمي
- الفصل بين الحسابات الشخصية والمهنية
- مراجعة إعدادات الخصوصية باستمرار
- الحذر من الروابط المجهولة والمرفقات المشبوهة
- استخدام كلمات مرور قوية ومتجددة

إطار حماية البيانات — ثلاثية السرية والسلامة والتوافر



إطار حماية البيانات الأكاديمي يركّز على ثلاثة مبادئ: **السرية**، (Confidentiality) السلامة/السلامة المعلوماتية **Integrity** والتوافر. (**Availability**) تطبيق هذه الثلاثية يتطلب سياسات وصول، آليات تشفير، وإجراءات نسخ احتياطي واستعادة.

الحفاظ على السرية يعني منع الاطلاع غير المصرح به؛ السلامة تعني عدم تعديل البيانات بغير إذن؛ التوافر يعني وصول مصرح عند الحاجة.

تطبيقات السلامة المهنية في الإعلام



✓ حفظ نسخ احتياطية من المواد الصحفية

✓ استخدام شبكات VPN عند العمل من أماكن عامة

✓ التأكد من صحة المصادر الرقمية قبل النشر

✓ التبليغ الفوري عن محاولات اختراق أو انتهاك

أمثلة مهنية:

في عام 2020، تعرّضت حسابات عدد من الصحفيين والناشطين في إكس تويتر انداك لهجمات "تصيد" استهدفتهم برسائل تبدو من "التحقق الأزرق"، ما أدى لاختراق حساباتهم ونشر محتوى مزيف.

إدارة الأزمات الرقمية — خطوات أولية

عند اكتشاف حادث أمني:

➤ عزل النطاق المتأثر

➤ وقف الانتشار (قطع الوصول)

➤ استدعاء فريق الاستجابة

➤ تقييم الضرر

➤ إصدار بيان مبدئي داخلي وخارجي بحسب الخطة، الشفافية المنضبطة تُقلّل الضرر على السمعة.

مثال: بيان من المؤسسة يوضح أن التحقيق جارٍ ويطلب الصبر دون الإفصاح عن تفاصيل حساسة.

• تدريب المحاكاة واختبارات التصيّد

نفذ محاكاة هجمات التصيّد وعمليات اختبار اختراق أخلاقية لتعرّف نقاط الضعف البشرية والتقنية. قس مؤشرات الأداء

مثل نسبة الإجابة على رسائل التصيّد وزمن الاستجابة للحوادث. التدريب المتكرر يخفض الأخطاء البشرية.

البصمة الرقمية والهوية الرقمية وبناء السمعة على المنصات

السمعة الرقمية

السمعة الرقمية (Digital Reputation) هي التقييم العام الذي يُكوّنه الجمهور والمختصون والخوارزميات عن كيان رقمي استنادًا إلى المحتوى، التفاعلات، والتغطية الإخبارية.

السمعة تتأثر بسرعة بالحوادث الرقمية وتتطلب إدارة استباقية ومستمرة للحفاظ على المصداقية.

إدارة السمعة الرقمية

- ✓ الالتزام بأخلاقيات النشر والمسؤولية في التفاعل
- ✓ مراقبة الإشارات والمشاركات التي ترتبط بالاسم المهني
- ✓ الرد الاحترافي على النقد أو الشائعات دون انفعال
- ✓ بناء محتوى إيجابي ومتسق مع القيم المهنية

الهوية الرقمية

الهوية الرقمية (Digital Identity) هي التجميع المنظم للسمات والبيانات التي تُعرّف كيانًا إلكترونيًا: أسماء المستخدمين، عناوين البريد، السمات البيومترية المحتملة، القرارات الخوارزمية حول الملف الشخصي، والعلاقات الشبكية. الهوية الرقمية تتبلور عبر المحتوى والسلوك وتُستخدم للتحقق، التفويض، وتخصيص الخدمات.

مثال: حساب منصة مهنية يمثل مؤسسة إعلامية يحمل شعارًا، وصفًا رسميًا، وربطًا بموقع إلكتروني مؤسسي.

<https://www.alarabiya.net>

تصفح قنوت



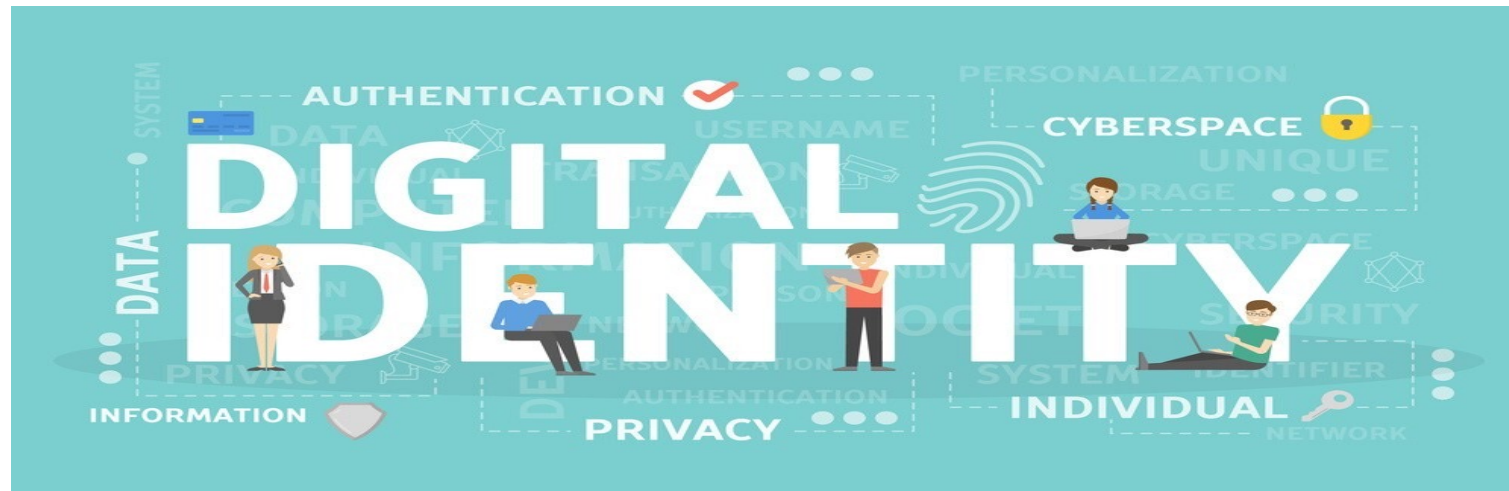
العربية
alarabiya

أمثلة تطبيقية

1. BBC تفرض على صحفييها قواعد صارمة لإدارة حساباتهم الشخصية منعًا لتضارب الآراء مع سياسة المؤسسة.

2. شركات التسويق العالمية مثل HubSpot تدرب موظفيها على بناء هويات رقمية متوافقة مع فلسفة العلامة التجارية.

سؤال تفاعلي: كيف يمكن للمسوق الرقمي أو الصحفي أن يحافظ على هويته الرقمية من التشويه أو السرقة؟



تقييم البصمة الرقمية

راجع ظهورك الرقمي عبر محركات البحث، تحقق من نتائج البحث الأولى، راجع الصور القديمة والمنشورات، وأعد ضبط إعدادات الخصوصية على الشبكات الاجتماعية. أدوات المراقبة والتنبيه تساعد على اكتشاف ذكر العلامة التجارية فورًا. أدوات مقترحة: أنظمة تنبيه البحث و Google Alerts للتحقق الدوري.

4 Types of Digital Footprints



Passive Digital Footprint

Website cookies, Browsing history, Shopping history, Background collection



Active Digital Footprint

Social media posts, Online publications, Public reviews, Deliberate sharing



Positive Digital Footprint

Professional achievements, Community involvement, Positive contributions, Reputation building



Negative Digital Footprint

Controversial posts, Negative reviews, Unprofessional behavior, Context-dependent

Dos and Don'ts When Responding to Negative Feedback

7 Simple tricks to start using now

1

Never Take Negative Feedback Personally

2

Never Argue With the Customer and Always Apologize

3

Acknowledge the Issue Quickly

4

Keep the Response Short Then Take It Offline

5

Always Personalize Your Response

6

Follow Up With Your Customers After You've Provided a Solution

7

Keep the Response Targeted to the Customer and Avoid Using Phrases "I think/feel"



الهوية الرقمية تُبنى عبر الاتساق في الرسائل، نبرة الصوت، الهوية البصرية، وجود صفحات رسمية متوثقة، وممارسات محتوى متسقة.

دليلاً صوتياً ومحتوى يحدد من سيكون المتحدث الرسمي وكيفية الرد على الأزمات. الاتساق يبني الثقة ويقلل التباس الجمهور.

مثال: قالب منشور رسمي موحد لكل الإعلانات المؤسسية.
إدارة التفاعل والردود السلبية

عند مواجهة تعليق سلبي، اتبع بروتوكول الرد:

تقييم الموضوعية، الرد بسرعة ضمن إطار مهني، الاعتذار عند الخطأ، وتقديم خطوات تصحيحية.

تجنّب الحذف العشوائي للمحتوى أو الدخول في سجالات قد تؤزم السمعة.
نموذج: ثلاث خطوات للرد: الاعتراف، التوضيح، التعهد بالإصلاح.

تحديات الامن السيبراني المحلية والإقليمية في سياقنا

التحديات قد تشمل:

✓ ضعف البنية التحتية للإنترنت

✓ نقص الموارد التقنية

✓ اختلاف الأطر القانونية لحماية البيانات

✓ الضغط السياسي الذي يؤثر على سياسات الحماية

الحلول تحتاج تكييف السياسات مع الواقع المحلي وبناء شراكات تقنية وتدريبية.

مثال: أزمة اختراق الشركات الخاصة في الأردن تهدد التحول الرقمي

تقرير إخباري- تفاجأ مالك شركة خاصّة تقدم خدمات تكنولوجيا مالية في عمان باختفاء بيانات شركته، قبل أن تصله رسالة تهديد تفيد بطلب فدية بقيمة 0.3 من عملة البيتكوين، بما يقارب 8 آلاف دينار.

يوثق هذا التقرير تعرض مواقع شركات خاصة في الأردن لخطر الاختراق وسرقة بياناتها وعملائها. فكيف يمكن صدّ الاختراقات وفق إجراءات وقائية عبر تفعيل قانون الأمن السيبراني وإقرار قانونٍ لحماية البيانات الشخصية.

<https://www.royanews.tv/news/304439>



اختراق وسرقة البيانات- صورة تعبيرية



أزمة اختراق الشركات الخاصة في الأردن تهدد التحول الرقمي

نشاط — تقييم حساسية مصدر

قم بتصنيف ثلاثة مصادر مفترضة (مرتبط بمعلومة حساسة، معلومة عامة، وشاهد عيان) من حيث الحساسية وخيارات الحماية اللازمة. ناقش الاختلافات في النهج الأمني لكل حالة.

أهداف النشاط: ربط الأمن الرقمي بالأخلاقيات المهنية.

نوع المصدر	درجة الحساسية	وصف موجز	آلية التعامل الفورية
مصدر داخلي مطلع على معلومات سرية	عالية (5/5)	موظف أو مطلع يملك وثائق سرية أو بيانات يمكن أن تسبب ضررًا مؤسسيًا أو قانونيًا إذا انكشفت	تواصل مشفر؛ عدم تخزين بيانات تعريف غير مشفرة؛ تشفير الوثائق؛ استشارة قانونية؛ حذف السجلات غير الضرورية
(Whistleblower) مبلغ عن فساد)	عالية (5/5)	شخص يقدم معلومات عن فساد أو انتهاكات قد تتسبب بملاحقة أو انتقام ضده	حماية هوية القطاع؛ قنوات اتصال مشفرة؛ تقييم مخاطر انتقام؛ تخطيط لنشر مشفر أو مؤجل
مصدر متعاون غير رسمي (محادثات خلفية)	متوسطة-عالية (4/5)	يزود معلومات غير موثقة رسمياً لكنه يقدم رؤى مهمة قد تكون حساسة	تحقق مستقل؛ تسجيل موافقة على مستوى الكشف؛ تشفير محتوى الاتصالات؛ تقييد الوصول
شاهد عيان لواقعة	متوسطة (3/5)	حضر حدثاً ويمدّ وصفاً للوقائع غالباً بدون تبعات قانونية مباشرة	توثيق، اقتراح نشر بلقب أو مجهول حسب الرغبة، التحقق من التفاصيل عند الإمكان
خبير أو محلل يقدم بيانات تفسيرية	منخفضة-متوسطة (2/5)	يوفر تحليلاً أو تعليقاً عاماً عادةً لا يعرض أحداً للخطر	توثيق المصدر، اقتباس بدقة، لا حاجة لتشفير ما لم يتضمن معلومات حساسة
معلومات حكومية منشورة رسمياً	منخفضة (1/5)	بيانات وإحصاءات منشورة في سجلات عامة أو بيانات المؤتمر الصحفي الرسمي	توثيق المرجع ورابط المصدر، تحقق من النسخة الأحدث قبل النشر
محتوى مستخدم منشور على الشبكات الاجتماعية	متغير (1-4/5)	منشورات عامة قد تصبح حساسة إن رُبطت بأشخاص محددين أو محتوى محمي	تحقق من السند الأصلي؛ احرص على إزالة بيانات تعريفية قبل إعادة النشر إن لزم
معلومات صحية أو شخصية عن فرد خاص	عالية (5/5)	بيانات طبية أو جنائية أو تعريفية قد تضر بالفرد عند النشر	تعامل كمصدر حساس؛ موافقة صريحة؛ تشفير؛ استشارة قانونية وأخلاقية

نموذج بريد إلكتروني احتيالي

From: updates@newsroom-secure.com

To: editor@mediaorg.org

Subject: **Urgent:** Verify your account to avoid suspension

Date: 12 Oct 2025 09:14 GMT

Dear Editor, Our security system detected unusual login attempts on your account. Please verify your credentials immediately to avoid suspension. Click the link below to confirm and update your password:

<http://bit.ly/verify-mediaorg>

If you do not act within 24 hours, access will be restricted.

Regards, Security Team — MediaOrg

✓ لا تنقر على الرابط؛ مرّر مؤشر الفأرة فوق الرابط لتظهر الوجهة الحقيقية قبل النقر

✓ تحقق من عنوان المرسل بدقة ومقارنته بقائمة العناوين الرسمية للمؤسسة

✓ ابحث عن مؤشرات الاستعجال والتهديد، الأخطاء اللغوية، وغياب معلومات تواصل رسمية

✓ الإجراء الأول: التقاط صورة للشاشة أو حفظ البريد وإرساله فورًا إلى فريق تقنية المعلومات مع عدم الرد

قائمة مؤشرات البريد الاحتيالي التي يجب الانتباه لها

1. اختلاف عنوان المرسل الظاهر عن عنوان النطاق الرسمي للمؤسسة (مثال: @newsroom-secure.com بدل @mediaorg.org).
2. وجود روابط مختصرة أو روابط لا تطابق النطاق الرسمي؛ مرر فوق الرابط دون النقر لرؤية الوجهة الحقيقية
3. نبرة استعجال غير مبررة تهدد بالإيقاف أو العقوبة الزمنية
4. أخطاء لغوية أو صياغية ركيكة في البريد الرسمي
5. طلب بيانات سرية عبر رابط أو مرفق (كلمات مرور، رموز تحقق، ملفات الدفع)
6. مرفقات بامتدادات قابلة للتنفيذ (.scr, .exe) أو ملفات مضغوطة غير متوقعة
7. غياب توقيع رسمي أو معلومات تواصل يمكن التحقق منها (هاتف داخلي، اسم مسؤول معروف)
8. عدم وجود شهادة أمان HTTPS حقيقية عند فتح الرابط أو شهادة غير صالحة
9. إرسال إلى قائمة توزيع واسعة غير مرتبطة بالموضوع (Cc/Bcc غير ضرورية)
10. اختلاف توقيت الإرسال أو توقيع إلكتروني لا يتطابق مع السجلات المؤسسية

مثال : مؤسسات حقوقية عربية

- [دليل-الأمن-الرقمي-للصحفيين](https://rc-rl.org//للصحفيين-الرقمي-الأمن-دليل) <https://rc-rl.org//للصحفيين-الرقمي-الأمن-دليل>

المركز الاقليمي للحقوق و الحريات هي مؤسسة قانونية مصرية تأسست في يناير 2016 على يد مجموعة من نشطاء حقوق الانسان الشباب حيث تضم مجموعة من المحامين و الباحثين.

يسعى المركز للوصول إلى مجتمع منفتح وعادل يتيح حرية البحث عن المعلومات وخلق الأفكار وتلقيها والتعبير عنها وتبادلها مع الآخرين دون خوف أو تدخل ظالم من الدولة وذلك بتمكين أفراد المجتمع ومساعدتهم في الحصول على حقوقهم والتمتع بحرياتهم بتمثيل احتياجاتهم أمام الجهات المسؤولة والتأكيد على ضرورة الالتزام بحقوق الانسان وسيادة القانون.



دراسات عربية في الامن السيبراني

<https://study.sa/> / [المجلات-العربية-للأمن-السيبراني](https://study.sa/)

الأمن السيبراني أصبح أحد المجالات الحيوية في العصر الرقمي، ومع ذلك، يبقى الوصول إلى مصادر متخصصة باللغة العربية تحديًا. تسعى العديد من المجلات العربية لسد هذه الفجوة، من خلال تقديم محتوى غني ومفيد. الدكتور ه حصة العمري قائمة بإعداد مقال يضم كل المجالات الأكاديمية الموثوقة الت يتوفر معلومات ودراسات موثقة وشاملة للباحثين والمهتمين في هذا المجال تجدونها في الرابط المرفق.

أجمل المجلات
العربية
للأمن السيبراني

المقال أهم المجلات والمصادر الرقمية العربية التي تعنى بموضوعات الامن السيبراني والعديد من النقاط الأخرى المهمة للباحثين والمهتمين في هذا المجال ستجدونها عبر الرابط المرفق

نشاط تطبيقي مقترح- غير إلزامي

تحليل حالة واقعية لاختراق أو تشويه سمعة رقمية لإعلامي أو مؤسسة إعلامية أو تسويقية.

قم بتحديد:

- نوع الخطر السيبراني الذي حدث.
 - أثره على السمعة أو المصداقية.
 - الإجراءات الوقائية التي كان يجب اتباعها.
 - توصيات لتعزيز الأمن الرقمي في حالات مشابهة.
- يُقدّم التحليل في عرض شفهي قصير خلال الجلسة النقاشية القادمة.

- Regional Centre for Reporting and Local. (2024). دليل الأمن الرقمي للصحفيين. <https://rc-rl.org/%D8%AF%D9%84%D9%8A%D9%84-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A/>
- <https://drasah.com/Description.aspx?id=8503> العفيفي، طارق. (2024). أفضل 10 ممارسات عربية متخصصة في الأمن السيبراني للمؤسسات الإعلامية. دراسة.
- المجلات العربية للأمن السيبراني: دلائل ومصادر للتعليم والتطبيق. (2024). Study.sa. <https://study.sa/%D8%A7%D9%84%D9%85%D8%AC%D9%84%D8%A7%D8%AA%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9-%D9%84%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A/>
- CNN Arabic. (2025, June 18). الشرك الأمنية تحت وابل من الهجمات السيبرانية المتعددة لعلامات إعلامية. <https://cnnbusinessarabic.com/technology/1120881/>
- Alborsa News. (2024, September 22). 70% من المواقع العربية تعرضت لهجمات سيبرانية خلال سنوات قليلة. <https://www.alborsaanews.com/2024/09/22/1827902>
- Roya News. (2023, July 20; updated 2024, August 30). ازمة اختراق المواقع الخاصة في الأردن تهدد التحول الرقمي. <https://royanews.tv/news/304439>
- Freedom of the Press Foundation. (2024). The journalist's digital security checklist. <https://freedom.press/digisec/blog/journalists-digital-security-checklist/>
- Center for News, Technology & Innovation. (2024). Journalists & cyber threats — Issue primer. <https://cnti.org/article/journalists-cyber-threats/>
- OWASP Foundation. (2023). OWASP Top Ten Web Application Security Risks. <https://owasp.org/www-project-top-ten/>
- Singer, N., & Perlroth, N. (2016). Blackout: How a Computer Virus Crashed the World's Power Grid. Crown.
- West, D. M. (2018). Data-Driven Journalism: A Practical Guide. Tow Center for Digital Journalism, Columbia University.
- Marwick, A., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051–1067. <https://doi.org/10.1177/1461444814543995>
- Rosen, J., & Gellman, R. (2014). Tools for source protection and secure communications. Journal of Digital Security Practice, 5(2), 45–62.



نلتقي في المحاضرة القادمة .. دمتم بخير