رقميّون

الخصوصيـــــــة والسلامة الرقمية

مارس 2026

رقميّون

المقدمة

لم تعد الخصوصية الرقمية مجرد رغبة في "إخفاء" المعلومـــــات، بل أصبحت مفهومًا جوهريًا يتمحور حول حوكمة العلاقـــة بين الفرد وبياناته في الفضاء السيبراني، وعملياً، لم تعد حماية الخصوصية "رفاهية"، بل ضرورة اقتصاديـــة حتمية. تشير الأرقام إلى أن الفشل في حماية البيانات يحمل فاتورة ضخمة على مستوى العالم قفز متوسط تكلفـة خرق البيانات ليصل إلى 4.88 مليون دولار في عام 2024، وإقليمياً بلغت تكلفـة الخرق في الشرق الأوسط ذروتها عند 32.8 مليون ريال (2024)، قبل أن تسجل تراجعاً طفيفـاً في 2025، وسجلت مدفوعات الفدية بالعملات الرقمية مستوى قياسيـــــــــاً تجاوز 1.25 مليار دولار في 2023، مما يعكس شراسة الهجمات السيبرانية عالمياً.

يعرف تقرير: **"الخصوصية والسلامة الرقمية"** بأهمية الخصوصية الرقميـــة في كونها حائط الصد الأول لحماية استقلاليـــة الفرد وتنوع أفكاره؛ فهي تمنع التلاعب بالسلوك البشري وتصون السمعة المؤسسية. في عالم الأعمال، الخصوصيـــــــــة هي "عملة الثقة"؛ فبدونها لا يمكن بناء علاقة مستدامـــة مع العملاء في سوق تنافسيـــة شديدة الحساسية.

فريق العمل

الخصوصيـــــة
والسلامة الرقميـــــة

2026
مـــارس

رقميّون

الخصوصية الرقمية

حماية بيانات المستخدمين على شبكة الإنترنت، وهو إحدى الحقوق التي أصبحت الكثير من المؤسسات ذات الشأن تدعو لضرورة تطبيقها حتى يستطيع المستخدم أن يتصفح الإنترنت دون قلق من إمكانية سرقة بياناته واستخدامها سواء إيجابيًا -استهداف المستهلكين لشراء منتج بعينه حسب تفضيلاتهم واهتماماتهم والمعلومات التي يبحثون عنها – أو سلبيًا -سرقة تلك البيانات لابتزاز أصحابها بغرض الحصول على المال أو حتى استغلالها من قبل الجهات السيادية لتوجيه الناخبين أو مراقبة بعض الشخصيات وهكذا

أنواعها

البيانات الشخصية

- وهي أي معلومات تتعلق بشخص مُعرّف أو قابل للتعرّف عليه، وتشمل بيانات الموقع والمعرّفات الرقمية

بيانات الموقع

- تبدو محايدة؛ ولكنها تكشف أنماطاً شديدة الحساسية (المنزل، العمل، الزيارات الطبية، وغيرها)

البيانات المالية

- وتشمل طيفاً واسعاً (حسابات بنكية، معاملات، سلوك إنفاق، منتجات ائتمانية)، وتُضمَّن معها عناصر مثل اسم حامل البطاقة وتاريخ الانتهاء

بيانات الأطفال

- تضاف إليها اعتبارات الأهلية الرقمية وتفاوت الإدراك بين الفئات العمرية، لأن الطفل قد لا يدرك عواقب الإفصاح أو المشاركة أو التتبع

البيانات الصحية

- تمتاز بأن أثر تسريبها يتجاوز الخسارة المالية إلى وصمة اجتماعية وتمييز، ولذلك تُعامل على نطاق واسع كبيانات حساسة

بيانات الشركات

- الشركات وتشمل أسراراً تجارية، ملكية فكرية، بيانات عملاء وموردين، سجلات تشغيل، وبيانات تشغيلية في القطاعات الصناعية، والخطورة فى تسريب البيانات

البيانات السلوكية

- تُبنى من التفاعل: ما الذي تنقر عليه، مدة البقاء، ترتيب الاهتمامات، أنماط التصفح، وتفضيلات المحتوى، القيمة الاقتصادية لهذه البيانات عالية لأنها تُستخدم للتخصيص والتوصية والتنبؤ، وخطورتها هنا فى الاستنتاجات التي يمكن استخراجها عبر التحليل وربط البيانات

رقميّون

أهمية الخصوصية الرقمية

01

- الأهمية الحقوقية، حقاً إنسانياً أصيلاً يتأثر مباشرةً بتوسع جمع البيانات وتحليلها، وهو ما أكدته قرارات دولية حول "الحق في الخصوصية في العصر الرقمي

02

- الأهمية المرتبطة بثقة المستخدم هي "عملة الاقتصاد الرقمي" حين يشعر المستخدم أن الخدمة تتجاوز الغرض أو تجمع بيانات أكثر مما يلزم أو لا توفر شفافية، تنخفض معدلات الاعتماد والاحتفاظ، وتزداد الحساسية لأي حادث

03

- الأهمية الأمنية، تتضح لأن الخصوصية من دون أمن تصبح وعداً غير قابل للتحقق، وأي نظام لا يستطيع منع الوصول غير المصرح به سيحوّل البيانات إلى مادة قابلة للسرقة

04

- الأهمية الاقتصادية، تتجسد في تحوّل البيانات إلى أصل إنتاجي وفي الوقت نفسه إلى مصدر تكلفة/مخاطر

رقميّون

الفرق بين

الخصوصية الرقمية والسلامة الرقميـــــة

الخصوصية الرقمية تركز على السيطـــرة المشروعة على البيانات وتقليـــــــل استخدامها غير الضروري.

السلامة الرقمية تركـــز على منـــع الأذى (اختراق، ابتزاز، خداع، برمجيـــات خبيثة، تنمر) والاستجابة للحوادث

أدوات التنفيذ غالباً مشتركة تشفير، ضبط صلاحيات حوكمة بيانات، واستجابة للحوادث، وتتمثل من خلال

الطبقة التقنية

- التشفير أثناء النقل وعند التخزيـــــن وتقنيات إدارة المفاتيح، إضافـــــة إلى الفصل بين البيانات والمعرفـــات ترميز أو إخفاء الهوية عند الإمكان
- هي مفاهيم تتبناها اللائحة التنفيذيـــة السعودية عبر تعريف "الترميز" و"إخفـــاء الهوية" كآليتين لتقليل إمكانية تحديـــد الهوية

طبقة السياسات والحوكمة

- اللائحة التنفيذية السعودية تُلزم جـهـــة التحكم بإبلاغ صاحب البيانات قبل أو عند الجمـع عن الغرض والمسوغ، ومدة الاحتفاظ، وحقـوق صاحب البيانات وآلية ممارستها، وإمكانيـــة العدول عن الموافقة، وتتضمن التزاماً بسجلات أنشطـــــة المعالجـــة ومدة الاحتفاظ بالسجلات وإتاحتها للجهة المختصة عند الطلب
- تقليل البيانات، تحديـــــــد الغرض، إدارة الاحتفاظ والإتلاف، وسجلات أنشطة المعالجة

رقميّون

طبقة الهوية والوصول

- التحكم بمن يستطيع الوصول إلى البيانات وتعزيز المصادقة متعددة العوامل وإدارة الهويـــة على مستوى المؤسسة

طبقة التطوير الآمن

- الخصوصية بالتصميم" و"الأمن بالتصمـــيـــم"، وهي مقاربة تبنّتها الأعمال الأكاديميـــــــة" والتنظيمية بوصفها انتقالاً من معالجة لاحقة للمشكلات إلى تضمين الوقايـــــــــة في التصميم

بناء اقتصاد رقمي قوي يتطلب بنية تحتية آمنة وثقة رقمية عاليـــة

الدكتور عبدالله السواحة
وزير الاتصالات وتقنية المعلومات

الاختراقـات السيبرانيـــة محلياً وعالميًا

عالمياً

- قفز متوسط تكلفة خـــرق البيانـــــــات ليصـــــــل إلـــــــى 4.88 مليـــــون دولار فـــــــي عام 2024 وفقاً لتقاريـــــر IBM

إقليمياً

- بلغت تكلفة الخرق فـــي الشرق الأوسط ذروتها عند 32.8 مليون ريال (2024)، قبل أن تسجل تراجعـــاً طفيفاً في 2025 بفضـــل تبني تقنيات التشفيـــر ومنهجيـــــــات (DevSecOps)

خسائر الفدية

- سجلت مدفوعات الفدية بالعملات الرقمية مستوى قياسياً تجاوز 1.25 مليار دولار فـــــي 2023، مما يعكس شراسة الهجمات السيبرانية

رقميُّون

عالميًا

15+
مليون حادثة جرائم إلكترونية عالمياً عام 2024

تسجيل
19.23 مليون حادثة عـــام 2021

38%
منها هجمـــــــات التصيد الاحتيالي

16%
هجمـــــــات الابـــتـــــزاز

+2,200
هجـــــــــوم سيبرانى يوميًـــا حـــول العالم

كل 39
ثانية يحـــــــدث هجـــــــوم سيبرانى

+2,000
حادثة جريمة إلكترونيـــة مُبلّغ عنها يوميًا الولايـــات المتحدة

32%
من المؤسسات العالمية عـــام 2025 تعرّضت لهجمات برامج الفديـــــة بسبب استغلال الثغرات الأمنية

813.55
مليون دولار مدفوعـــــــات برامـــــــج الفديـــــة عام 2024

متوسط تكلفة خرق البيانات بدولار

4,35	4.45	4.88
عام 2022	عام 2023	عام 2024

مدفوعات الفدية بالعملات الرقمية

765.6$	1.25B	456.8$	813.55$
عام 2021	عام 2023	عام 2022	عام 2024

رقميّون

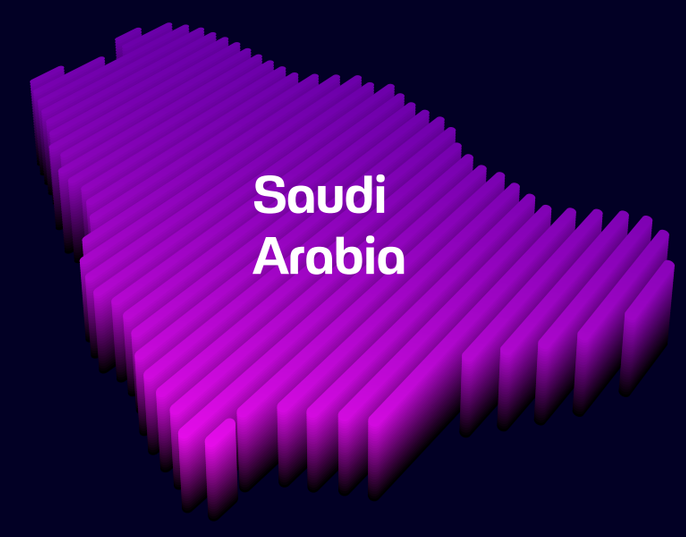
الأرقـــام سعوديًا

270+

- ألف هجـــــوم في النصف الأول من عـــــام 2025 بمعدل هجوم كل 90 ثانية

الرقم

- الأعلى فى الشرق الأوســـط ومن بين الأكبـر على مستوى العالم



22.5

- مليون هجوم إلكترونى فـــى عام 2020 وقدرت الخسائـر بـ 6.5 مليون دولار

وهو

- ما يجعل المملكة فى موقـع الصدارة كأحد الخطـــوط الأمامية الرقمية عالمياً

300

ألف هجمة سيبرانية يوميًا متوسط عدد الهجمات السيبرانية التي تم التصدي لها فى عام 2021م

من حيث حجم الاستهـــداف الأمنى الرقمي حسب شركـــة مايكروسوفت تعد السعوديـة

5
إقليميًا

23
إقليميًا

الخصوصيـــــة
والسلامة الرقميـــــة

2026
مـــارس

رقميّون

أنواع المخترقين إلى يقسمون إلى ثلاث فئات

قراصنة القبعة البيضاء

هم "الأخيار"

- يخترقون مواقع الشركات الإلكترونية أو بنيتها التحتية، ولكن بدلاً من استغلال الثغرات التي يكتشفونها، يبلغون الشركة عنها لإصدار تحديثات أمنية

عادةً

- ما توظف الشركات قراصنة القبعة البيضاء، أو قد يعملون من خلال برامج مكافآت اكتشاف الثغرات وتقدم الشركات مكافآت مالية لمن يكتشف ثغرة أمنية

قراصنة القبعة السوداء

هم

- على النقيض تمامًا فهم "الأشرار"، إن صح التعبير، إذ يخترقون الأنظمة بشكل غير قانوني لتحقيق مكاسب شخصية

يستغلون ثغرات

- الأنظمة للعثور على معلومات شخصية لسرقتها، أو مجموعات بيانات لتسريبها مما يؤدي إلى اختراقات أمنية

قراصنة القبعة الرمادية

لا يلتزم

- قراصنة القبعات الرمادية بالمعايير الأخلاقية أو حتى القوانين عند القرصنة، لكن الكثير منهم يعتقدون أن ما يفعلونه ضروري لجعل الإنترنت – والعالم – أكثر أمانًا

عادةً

- لا يقصدون إلحاق الضرر، على الأقل بالجمهور، لكن عالم الأمن السيبراني ينظر إلى أساليبهم على أنها غير أخلاقية

رقميّون

أنواع عمليات المخترقيـــــن

الاختراقات غير المعروفة

- عادةً ما يلجأ المخترقون إلى هذه الاختراقات لاستهداف الشركـــــات التي يمكنهـم تحقيق مكاسب شخصية منها، سواء كانت شركات دولية أو أنظمة أمن قومي
- تشمل ثغــرات أمنية لم يسبق للشركة أن واجهتها. بل قد لا تكون الشركة على دراية باختراقها أصلاً

أنواع الاختراقات المتنوعة

- تستخـــــــدم معظم أنواع الاختراقات الأخرى ما يُعرف ببرامج الاختراق الجاهزة، وهي برامج موجودة مسبقًا لا تتطلب معرفة برمجية كبيرة لمهاجمة النظام
- على عكس اختراقات اليوم الصفر، يسهل على الأنظمة حماية نفسها من برامج الاختـــــراق الجاهزة إذا تم تحديث البرنامج

كيـــــف تمم عملية الاختراق

الهندسة الاجتماعية

- وهي من أسهل الطرق لاختـــراق حساب أو نظام وطلب من المستخدم كلمة مروره قد يتخذ هـذا شكل التصيد الاحتيالي أو المكالمات الهاتفيـــة المزعجة، لذا كن حذرًا عند مشاركـــــة بياناتك الشخصية

القرصنة

- القائمة على البرمجة تتطلب من المخترق إيجـــاد نقاط ضعف في النظام والاستيلاء على جميـــع الامتيازات الإدارية

يمكن اختراق أي نظام - لم يعد سرًا

دان كامينسكي
باحث وخبير أمن سيبراني أمريكي

الخصوصية والسلامة الرقمية

2026
مارس

رقميّون

الأنظمة السعودية الحاميـــــة للخصوصية والسلامة الرقمية

تتبنى المملكة منظومة متعدة الطبقات تجمع بين تنظيم الخصوصية، وحوكمـــــة البيانات، وتنظيمات قطاعيـــــة، وأطر للأمن السيبرانى. هذه الطبقات تحتاج إلى تنسيق دقيق لتجنب التعارض وتوزيع الاختصاصات بوضوح، ومن يمكن حصر الأنظمة الراعية للخصوصيـــــة والسلامية الرقمية

نظام حماية البيانات الشخصية ولوائحه التنفيذية

- المرجعية الرسميـــــة المعروضة من الهيئـــة السعوديـــــة للبيانـــــات والذكاء الاصطناعى
- تؤكد أن النظـــام "يحمى البيانات الشخصية للأفـراد ويضمن حقوقهـــم ويحـدد التزامـــات المتحكمين
- تتضمن اللائحة التنفيذيـة نقاطاً تشغيلية شديـــدة الأهمية لأنها تتحـــول إلى "ما يجب فعله فعليـــاً" داخل المؤسسات

لوائح هيئة الاتصالات وتقنية المعلومات سابقاً والهيئة الحالية CST

- أصدرت هيئة الاتصالات والفضاء والتقنية وثيقة "القواعد العامة للمحافظة على خصوصية البيانات الشخصية للمستخدمين لقطاع الاتصالات وتقنية المعلومات
- تشير تنظيمات قواعد حماية المستخدم إلى حماية المستخدم ورفع مستوى الثقة عبر جودة الخدمات وتوفير الحماية من المحتوى الضار والحفاظ على سرية الاتصالات
- على مستوى السلامة/الأمن القطاعى، توجد أيضاً وثائق تنظيميـــــة مثل "الإطار التنظيمى للأمن السيبرانى" للجهات الخاضعة لتنظيم الهيئة فى قطاع الاتصالات والتقنية
- أدلة/ تنظيمات مرتبطة بإنترنت الأشياء تُظهر أن الخصوصية تُعامل كمتطلب تنظيمى ضمن بيئة إنترنت الأشياء

رقميّون

نظام مكافحة الجرائم المعلوماتية

- يؤدى نظام مكافحة الجرائم المعلوماتية وظيفة "ردعية/جنائية" تكمل منظومة الخصوصيــة فهو لا ينظم جمـــــــــع البيانات فقط، بل يجرّم أنماطاً مثل الدخول غير المشروع والتنصت والاعتداء على البيانات/الأنظمة

- فى النص الرسمى المنشور يظهر إطار العقوبات قد تصل إلى السجن والغرامة بحسب الفعل وخطورته

القراصنة لا يحتاجـــون إلى أسمـــاء أو قـــــرب جغرافى بل يحتاجـــون فقط إلى فرصة

كيفن ميتنيك
مخترق سابق وخبير أمن سيبرانى أمريكى

الخصوصيـــــة
والسلامة الرقميـــــة

2026
مـــارس

رقميّون

خصوصيـــــــة البيانات على منصات التواصل الاجتماعـــي

تحرص مواقع التواصل الاجتماعي وشركات المحمول على إضفاء صفة شرعية لاستخدام تلك البيانات من خلال نظام حماية خصوصية البيانات الشخصية، وطلب الإذن من المستخـــدم للسماح للتطبيق بتتبع نشاطه على الإنترنت، وفي حال رفض المستخدم ذلك من المفترض أن تتوقف عملية المراقبة والتتبع، ومنها :

استخدام ملفات الارتباط (كوكيز)

تسمح

- تسمح لأصحاب الموقع بمعرفة تجربـــة المستخدم وفترة بقائه في كل صفحـــة، وفترة تصفحه للموقـــع ككل، وبالتالـي استخدامها في أغـــــراض تحليليـــــة وتسويقية

لا تحتفظ

- تحتفظ باسم المستخدم ولا بياناته، فقط تحتفظ بملف تعريف جهازك، وموقعـــك على الخريطة، لديك الحريـــة في رفض أو قبول تلك الخاصية

WE ARE COOKIES?

ACCEPT

REJECT

يضم معلومات

- حول طرق جمع التطبيقات أو الموقع الإلكترونـي لبيانات المستخدمين، لذلك قبل النقر بالموافقة، عليك قراءة تلك الشروط حتى تضمن تجربة آمنة أثناء التصفح

سياسات الخصوصيـــة

الخصوصيـــــــة
والسلامة الرقميـــــــة

2026
مـــارس

رقميّون

الحق في رفض استخـــــدام بياناتـــــك الشخصية

بعض المواقع

- المواقع أضافت إمكانية المطالبة بالتراجـــع عن استخدام بياناتك، فحتى إن ضغطـــــت على زر الموافقة على سياسات الخصوصية، أو الموافقة على استخدام ملفات الارتباط، يظل لديك الحريـة فى التراجع عن هذا القرار ومطالبة الشركـــة بإزالة جميع بياناتك التى سُجلت تلقائيًا

وتعني حماية الخصوصية الرقمية

- حماية المعلومات الشخصية، تمثل البيانات الشخصية ذات قيمة هائلة لمجرمـــى الإنترنت، بدءًا من التفاصيل المالية وصولًا إلى عناوين المنازل
- الدفاع ضد التهديدات الإلكترونية، وتشمل التهديدات الإلكترونية طيفًا واسعًا من الأنشطـة والمخاطر الخبيثة التى قد تُعرّض أمنك الإلكترونى ومعلوماتك الشخصية للخطر
- حماية السمعة على الإنترنت، تُمكّنك حماية خصوصيتك الرقمية من التحكم فى المعلومات المتاحة عنك على الإنترنت

إذا كنت تعتقد أن التقنية وحدها ستحل مشكلاتك الأمنية، فأنت لا تفهم التقنيـة ولا الأمن

بروس شناير
خبير أمن سيبرانى وتقنى أمريكى مشهور عالميًا

الخصوصيـــــة
والسلامة الرقميـــــة

2026
مـــارس

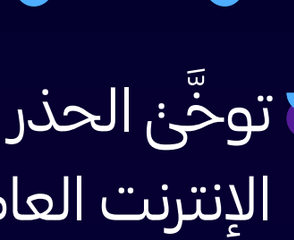
رقميّون

أفضل الممارسات لحماية الخصوصية الرقمية

- استخدم كلمات مرور قوية وفريدة

- تفعيل المصادقة متعددة العوامل

- تحديث البرامج وأنظمة التشغيل بانتظام



- توخَّى الحذر عند استخدام شبكات الإنترنت العامة

- تشفير البيانات استخدم أدوات التشفير، مثل BitLocker من مايكروسوفت و FileVault من أبل، لحماية بياناتك أثناء نقلها مثل HTTPS وعند تخزينها تشفير القرص بالكامل

- التنبه عند الموافقة على الشروط والأحكام وسياسات الخصوصية فمن السهل الموافقة على شروط وسياسات المواقع الإلكترونية المختلفة التى نزورها يوميًا دون قراءتها

الخصوصية والسلامة الرقمية

2026
مارس

رقميّون

تأثير الخوارزميات والذكـــــاء الاصطناعي على السلامـــــة الرقمية

- أثر الخوارزميات لا ينحصر في "جمع البيانات"، بل في "قدرة الاستنتاج حتى لو لم تُجمـــــع معلومة حساسة بشكل مباشر، قد يُستدل عليها من أنماط سلوكية، علاقات اجتماعية، موقع، أو تفاعلات محتوى. لذلك يصبح مفهوم "المعالجة الآلية واتخاذ القرارات" محوراً للشفافيـــة والحوكمة

- "يشير تقريـــــر تكلفـــة الخرق لعـــام 2025 إلى فجوة "حوكمة الذكاء الاصطناعـــي (AI oversight gap) وإلى أن تبني الذكاء الاصطناعي يتسارع أحياناً أســـــرع من تطبيق الأمنية والحوكمية الكافية، مع إبراز أثر ذلك على التكلفة والمخاطر

- في السياق التعليمي والاجتماعي، تنبّه UNESCO إلى أن الذكاء الاصطناعي والتقنيات الرقمية يجب أن تُستخدم بصورة متمحورة حول الإنسان ومرتكزة على الحقوق لا تتحول إلى عامـــل يهدد الحقوق الأساسية للمتعلمين

- تُربط المخاطر أيضاً بمسألة الحوكمة والرقابة على استخـــــدام الذكاء الاصطناعي داخل المؤسسات

الخصوصيـــــة
والسلامة الرقميـــــة

2026
مـــارس

رقميّون

ومن منظور الحماية الرقمية؛ من أبرز المخاطـــــر التي ينبغي الانتباه لها، والاعتبارات الواجب اتخاذهـــا قبل مشاركة أية معلومات شخصيـــــة أو صور عبر هذه التطبيقات

...

انتهاك الخصوصية

- عند رفع صورة شخصية أو معلومات شخصيـــــة في تطبيق ذكاء اصطناعي فإننا غالباً نمنح التطبيق صلاحية استخدام هذه البيانات
- بعض التطبيقات تحتفظ بالصور ومعلومات الوجه وتستخدمها لتدريب خوارزميات الذكـــاء الاصطناعي، أو حتى لأغراض تجارية دون علمنا أو موافقتنا الصريحة
- تنص بعض التطبيقات في شروط الاستخدام أنها تحتفظ بالحق في استخـــــــدام الصور والمعلومات المدخلة لأغراض "تحسين الخدمـــة" أو "التطوير"، وهي عبارات فضفاضة قد تعني أي شيء مثل تدريب النماذج إلى بيع البيانات
- يمكن أن تستخدم بانتحال الهوية، ومن الصعب جداً إزالتها بعد رفعها على تطبيقات الذكـــاء الاصطناعي

تطبيقات غير موثوقة أو تتبع لجهات مجهولة

- تطلب هذه التطبيقات صلاحيات واسعة دون مبرر (مثل الوصول للكاميرا، الموقع، وجهـــات الاتصال) مما يجعلها عرضة للاستخدام السيئ أو حتى تكون أدوات للتجسس وسرقة الهويـة أو حتى الابتزاز الإلكتروني

مخاطر التزييف العميق

- تُستخدم هذه التقنية للإساءة أو الابتزاز، خاصةً إذا كانت الصور الشخصيـــــة بحوزة جهات احتيالية، أو قد يؤدّي التزييف إلى نشر معلومات مضلّلة والتأثير على الرأي العام

رقميّون

الصور تتضمن معلومات أخرى

- تحتوي الصور على بيانات خفية (metadata) تحدد الموقع الجغرافي للصورة أو نوع الكاميرا أو معلومات متعلقة بالجهاز تاريخ ووقت التقاط الصورة

إقامة علاقات عاطفية مع تطبيقات الذكاء الاصطناعي

- تعمل تطبيقات الأصدقاء الافتراضيين والروبوتات الرومانسيّة وكأنها الرفيق الموثـــوق فيـه والذي يعرف كل شيء عن المستخدم ويهتم بشؤونه ويجمع أدق تفاصيل حياته التي يمكـن أن يتم استغلالها في حال حدوث اختراق أو تسريب بيانات

مخاطر في مجال التعليم

- فقدان مهـــارات البحث والتحليـــل مما يعرض الباحثين للخطأ إذا لم يتم التحقق من المصادر
- عندما يتم الاعتماد على النتائج المطلقة دون التفكير فيها ظناً أن الذكاء الاصطناعي لا يخطئ

الأمن السيبراني مسؤوليـــة الجميع، وليس مسؤولية قسمم تقنية المعلومات فقط

تيريزا بايتون
خبيرة أمريكية بارزة في الأمن السيبراني

الخصوصيـــة
والسلامة الرقميـــة

2026
مـارس

رقميّون

@Raqmyon

raqmyon.com

الشريك
الاستراتيجـــــــي

amaz
Marketing Solutions

المراجع