الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

السلامة الرقمية في الإعلام

الشريحة المستهدفة

الإعلاميون

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

مبادئ عامة في السلامة الرقمية

السلامة الرقمية في الإعلام

الشريحة المستهدفة

الإعلاميون

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 66 798
16555
academy@ncsa.gov.qa
00974 510 45 944

تمهيـــد

السَّلامة الرقميَّة ركيزة أساسيَّة لضمان أمْن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تم تصميم هذا الكُتَيِّب بهدف توعية الإعلاميين بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيِّب إلى تعزيز وعيهم بأبرز التهديدات السيبرانية التي قد يتعرَّضون لها في أثناء عملهم؛ مثل: التصيّد الاحتيالي، برمجيات الفدية، الفيروسات، الهندسة الاجتماعية، التزييف العميق، وسرقة الهوية الرقمية.

كما يُقدِّم الكُتَيّب أفضل الممارسات والإجراءات الوقائية لحماية الأجهزة، وتأمين الحسابات، والتعامل السريع مع مؤشرات الاختراق، وتأمين البيانات، وكيفية كَشْف الأخبار المُضلّلة والتعامل معها.

وتُعدّ هذه الجهود جزءًا من المبادرة الوطنية للسلامة الرقمية التي تُنظّمها الوكالة الوطنية للأمن السيبراني، لبناء بيئة رقمية آمِنَة لجميع فئات المجتمع.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

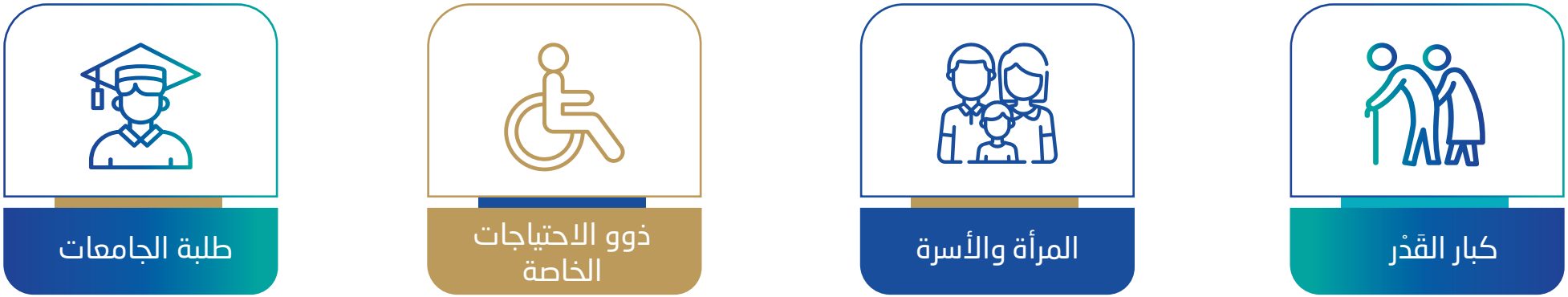
تعـــريف المبادرة

مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

وتعمل على نَشْر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومُتمكِّن تكنولوجيًّا.

الشرائح المستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها في السنة الأولى على الشرائح التالية:



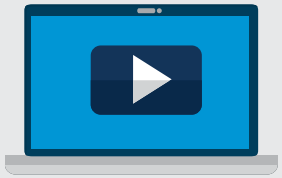
أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

دليل السلامة الرقمية

كتيبات توعية

ألعاب سيبرانية



فيديوهات توعية

ألعاب تعليمية مبتكَرة

ورش توعية

البرمجيات الضارّة

هي تطبيقات أو تعليمات برمجية ضارّة تستهدف الوصول غير المصرّح به إلى أجهزة الحاسوب أو الهواتف الذكية، بغرض خرقها، وسرقة البيانات المهمّة، وقد تتسبّب في إلحاق الضرر بها أو تعطّلها وخروجها عن العمل.

01

الفصل الأول

أساسيات السلامة الرقمية

مفهوم السلامة الرقمية

السلامة الرقمية هي مجموعة الإجراءات والممارسات التي تُمكِّن الإعلاميين من حماية بياناتهم الشخصية والمهنية عند استخدام الأجهزة والإنترنت.

السمات الأساسية للسلامة الرقمية للإعلاميين

- توفير الحماية للأجهزة من الاختراق والبرمجيات الخبيثة
- الحفاظ على سرّية مصادر المعلومات الصحفية
- ضمان سلامة المراسلات أثناء التغطيات والتحقيقات
- مَنْع الوصول غير المُصرَّح به للبيانات
- تعزيز الثقة بين الصحفي والجمهور من خلال بيئة رقمية آمِنَة

التهديدات الرقمية الشائعة

يتعرَّض الإعلاميون لأنواعٍ مختلفةٍ من الهجمات الرقمية التي تَهْدف للسرقة أو التشويه أو التضليل.

التصيّد الاحتيالي عبر البريد الإلكتروني والرسائل النصية

البرمجيات الخبيثة وبرامج الفدية

الهندسة الاجتماعية المبنية على الخداع

التنصّت على الاتصالات خلال استخدام شبكات عامة

التزييف العميق لإنتاج فيديوهات أو تسجيلات مُضلّلة

البرمجيات الخبيثة (Malware)

يقوم المهاجمون بإرسال البرمجيات الخبيثة إلى الأجهزة بهدف إلحاق الضرر، أو سرقة البيانات، أو التحكُّم في المحتويات.

السمات الرئيسية

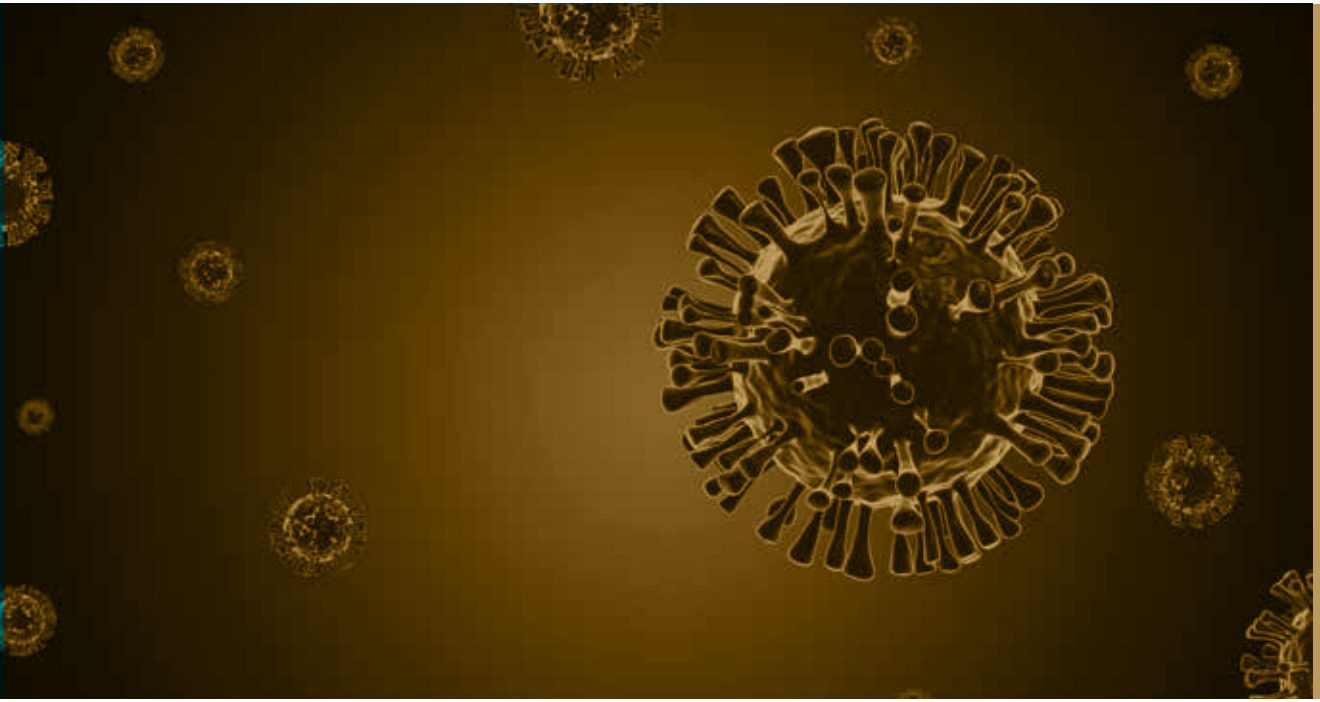
- تنتقل عبر المرفقات أو الروابط المشبوهة
- قد تُخْفِي نفسها داخل برامج أو تطبيقات ظاهرها سليم
- تتنوّع بين فيروسات، ديدان، برمجيات فدية، أو برمجيات تجسُّس
- تؤدي إلى فقدان السيطرة على الأجهزة أو البيانات
- تُستخدم أحيانًا للتجسُّس على عمل الصحفيين

طرق الوقاية

- تثبيت برامج مكافحة الفيروسات، وتحديثها بانتظام
- تجنُّب تحميل البرامج من مواقع غير موثوقة
- عدم الضغط على الروابط أو المرفقات المجهولة
- تشغيل جدار الحماية لصدّ الهجمات
- إجراء فَحْص دوري للجهاز للتأكُّد من خلوّه من البرمجيات الضارَّة

الفيروســـات

الفيروس هو برمجيَّة ضارَّة تَدخل إلى الجهاز وتُغيِّر طريقة عمله، أو تُتْلِف البيانات الموجودة عليه.



السمات الرئيسية

- يُرفَق غالبًا مع ملفات تبدو طبيعية مثل الصور أو المستندات
- يبدأ الفيروس بالانتشار عند فَتْح الملف أو تشغيله
- بعض الفيروسات تتسبَّب في حذف الملفات أو تعطيل النظام بالكامل
- ينتقل من جهاز إلى آخر عبر الإنترنت أو وسائط مثل USB

طرق الوقاية

- استخدام برامج مكافحة الفيروسات المُحدّثة باستمرار
- عدم فَتْح الملفات مجهولة المصدر
- فحص وسائط التخزين (USB) قبل تشغيلها
- تحديث أنظمة التشغيل والبرامج لإغلاق الثغرات الأمنية

برمجيـــات الفدية (Ransomware)

برمجيات الفدية هي أحد أخطر أنواع الهجمات؛ حيث يتم تشفير الملفات ثم يُطلَب دَفْع مبلغ مالي لفَكّ التشفير.

السمات الرئيسية

- تُرسَل عادة عبر رسائل بريد إلكتروني تحتوي على مرفقات مزيَّفة
- بعد الإصابة، تُغْلِق الملفات أو النظام بالكامل
- المهاجم يطلب فدية غالبًا بعُمْلة رقمية مثل البيتكوين
- حتى عند الدفع، لا يُوجَد ضمان لاسترجاع الملفات

طرق الوقاية

- النَّسخ الاحتياطي المنتظِم للملفات المهمة
- تجنّب فتح المرفقات من مصادر مجهولة
- استخدام برامج أمنية متخصّصة في منع هجمات الفدية
- تحديث النظام والتطبيقات باستمرار لسدّ الثغرات

التصيد الاحتيالي

التصيّد الاحتيالي هو محاولة خداع من خلال رسائل أو مواقع تبدو كأنها حقيقية، لكنَّها مُصمَّمة لسرقة المعلومات.

سمـــات رســائل التصيد الاحتيالي

- غالبًا ما تأتي على شَكْل رسائل بريد إلكتروني أو رسائل نصية
- تَطلب من المستخدم إدخال بيانات حسَّاسة مثل كلمات المرور أو أرقام البطاقات البنكية
- تَستخدم لغةً مستعجلة مثل "حسابك موقوف، تصرَّف الآن!"؛ لتحفيزك على التفاعل دون تفكير
- تُقلّد تصميم وشعارات مؤسسات معروفة لتبدو كأنها شرعية
- الهدف الرئيسي هو سرقة المعلومات لاستغلالها ماليًّا أو للابتزاز

طرق الوقاية

- التأكد من عناوين البريد والروابط قبل النقر عليها
- عدم مشاركة البيانات الشخصية عبر الرسائل المشبوهة
- استخدام خاصية التحقق بخطوتين للحسابات

الهندسة الاجتماعية

الهندسة الاجتماعية تعتمد على استغلال المشاعر البشرية لخداع المستخدِم، بدلًا من استخدام أدوات تقنية مُعقَّدة.

السمات الرئيسية

- يَستخدم المهاجم أسلوب الإقناع والتلاعُب النفسي للحصول على المعلومات
- قد يتظاهر بأنه مُوظَّف دعم فني، أو صديق، أو مسؤول
- يعتمد على جَمْع معلومات من مواقع التواصل لجَعْل المستخدِم يثق به
- يستغلّ مشاعر مثل الخوف، أو التعاطف، أو الحَرَج لدَفْعك للتجاوب
- تُعدّ من أخطر الوسائل؛ لأنها لا تحتاج مهارات تقنية، بل تعتمد على سلوك الضحية

طرق الوقاية

- التحقُّق من هوية المتصل أو المُرسِل قبل مشاركة أيّ معلومة
- تجنّب مشاركة تفاصيل حساسة مع أشخاص غير موثوقين
- توعية الفريق الصحفي بخطورة هذا الأسلوب
- اعتماد بروتوكولات واضحة للتحقُّق قبل الاستجابة لأيّ طلب

التزييف العميق (Deepfake)

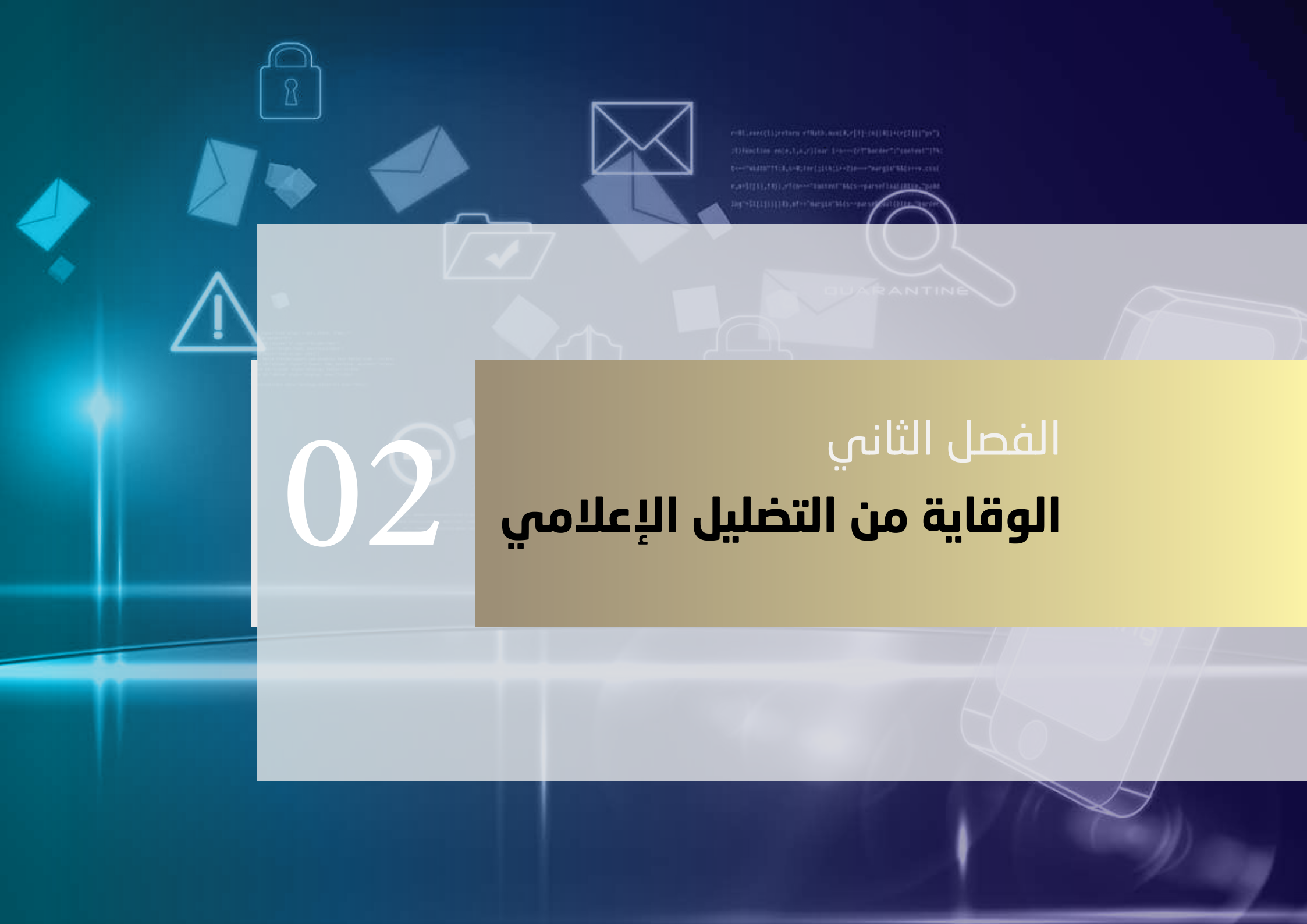
التزييف العميق هو استخدام الذكاء الاصطناعي لإنتاج محتوى مزيَّف بشكل قريب للواقع.

السمات الرئيسية

- إنشاء فيديوهات أو تسجيلات صوتية تُقلّد شخصيات عامة
- صعوبة التمييز بين الحقيقي والمزيَّف
- تهديد مباشر لسُمعة الصحفي أو المؤسسة الإعلامية
- يُستخدَم لنَشْر أخبار مُضلّلة تَستهدف الرأي العام

طرق الوقاية

- استخدام أدوات كشف التزييف العميق
- ملاحظة العلامات غير الطبيعية في الحركات أو الأصوات
- الاعتماد على مصادر متعدّدة قبل نَشْر أي محتوى مرئي أو صوتي
- التحقُّق من البيانات الوصفية (Metadata) للملفات الرقمية



02

الفصل الثاني

الوقاية من التضليل الإعلامي

مفهوم الأخبار المُضلّلة

الأخبار المُضلّلة هي محتويات إعلامية يجري إنتاجها أو نَشْرها بقَصْد الخداع أو إثارة البلبلة أو التأثير على الجمهور. وقد تكون مكتوبة أو مصورة أو مسموعة.

السمات الرئيسية للأخبار المُضلّلة

01 قد تكون مُلفَّقَة بالكامل، ولا صلة لها بالواقع

02 قد تُبنَى على وقائع حقيقية أُخرجت من سياقها

03 كثيرًا ما تلجأ إلى المبالغة في الأرقام أو الأحداث

04 غالبًا ما تُرْفَق بمصادر غامضة أو مجهولة

التحقُّق من الصور والفيديوهات

الصور والفيديوهات تُعتبر الأكثر استغلالًا في التضليل، خصوصًا مع تقنيات التعديل الحديثة.

طرق التحقُّق

- استخدام البحث العكسي عن الصور لتحديد أصلها وتاريخها
- استخدام أدوات موثوقة لتحليل الفيديوهات والكشف عن الإطارات والتفاصيل
- التدقيق في الظلال أو ملامح المكان لمطابقتها مع الحدث
- مقارنة المحتوى مع أكثر من مصدر موثوق

التزييف العميق والفيديوهات المُفَبْرَكَة

التزييف العميق أصبح أحد أخطر وسائل التضليل؛ نظرًا لصعوبة اكتشافه.

مؤشرات الكشف

- عدم تطابق حركة الفم مع الصوت في الفيديو
- تفاصيل بصرية غير طبيعية مثل الألوان أو الظلال
- غياب مصادر أصلية للمقطع أو نشره أولًا عبر قنوات مجهولة
- اقتصار الفيديو على نسخة واحدة رغم أهميته المُفتَرَضَة

دور وسائل التواصل الاجتماعي
في نشر التضليل

وسائل التواصل ساعدت على تسريع انتشار الأخبار الكاذبة بشكلٍ غير مسبوق.

أبرز سمات النشر عبر التواصل

- الاعتماد على **العناوين المثيرة** لجَذْب التفاعل دون التأكُّد من المضمون
- استخدام **الصور المُعدَّلة** والهاشتاغات لنشر الشائعة
- إعادة **نشر الأخبار بسرعة** من دون تحقُّق مسبق
- الاعتماد على «**الترند**» كدليل كاذب على المصداقية

خطوات الوقاية من الوقوع في التضليل

لتقليل الخطر من الوقوع في التضليل، هناك مجموعة من الإجراءات الوقائية الأساسية.

خطوات الوقاية

- عدم التسرُّع في نَشْر أيّ خبر قبل التحقُّق من صحته
- الاعتماد على مصادر متعدّدة ومتنوّعة قبل اعتماد المعلومة
- بناء شبكة من المصادر الموثوقة لتأكيد الأخبار
- توعية الجمهور بخطورة الأخبار المُضلّلة وآليات كشفها

التعامل مع مصادر مجهولة عبر الإنترنت

المصادر المجهولة قد تكون فرصة للحصول على معلومة مهمة، لكنّها في المقابل قد تُستغَل كأداة لتضليل الصحفي.

الوقـايــة

التأكُّد من الهوية الرقمية

استخدام أدوات تتبُّع البريد أو الحسابات؛ للتأكد من أصالة الجهة المرسِلة

التعامل عبر قنوات آمِنَة

الاعتماد على تطبيقات تَراسُل مُشفّرة عند الحاجة للتواصل

التحقّق المتقاطع

مقارنة ما يُقدّمه المصدر مع بيانات من مصادر أخرى موثوقة