كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

دليلك الشامل للحماية من الجرائم الإلكترونية

Your Comprehensive Guide to Cybercrime Protection

English

العربية

اضغط على الجريمة الإلكترونية لمعرفة التفاصيل:

- الابتزاز الإلكتروني
- التصيّد الإلكتروني
- التنمّر الإلكتروني
- اختراق الحسابات الشخصية
- البرمجيات الخبيثة
- انتحال الشخصية
- المواقع المزيّفة
- التزييف العميق

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

Click on any cybercrime to read the full details:

- Cyber Extortion
- Phishing
- Cyberbullying
- Account Hacking
- Malware
- Identity Impersonation
- Fake Websites
- Deepfake

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هو الابتزاز الإلكتروني؟

هو تهديد عبر المنصّات الرقمية لإجبارك على دفع المال أو تنفيذ مطالب معيّنة باستخدام صور أو معلومات شخصية حقيقية أو مُفبركة. غالباً يبدأ التواصل بشكل عادي ثم يتحوّل سريعاً إلى تهديد مباشر.

كيف تحمي نفسك؟

- لا تشارك صوراً أو معلومات شخصية عبر الإنترنت.
- فعّل إعدادات الخصوصية في جميع حساباتك.
- تجنّب الروابط والملفات المجهولة.
- استخدم كلمات مرور قوية ومختلفة لكل حساب.
- لا تثق بأي جهة تطلب منك محتوى شخصياً.

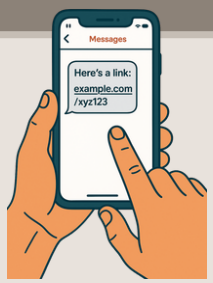
إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هو التصيّد الإلكتروني؟

هو خداع الضحية للحصول على بيانات حساسة عبر رسائل أو روابط تبدو وكأنها من جهة موثوقة.
يستهدف المهاجم إقناع الضحية بالنقر وإدخال بياناتها في صفحة مزيفة، وقد يحدث ذلك عبر البريد الإلكتروني أو الرسائل أو مواقع التواصل أو رموز الاستجابة السريعة (QR).



كيف تحمي نفسك؟

- لا تفتح أي رابط مجهول أو غير رسمي.
- تأكّد من صحة الرابط قبل الضغط عليه وتجنّب الروابط المختصرة.
- استخدم التطبيقات الرسمية للخدمات الحساسة مثل البنوك.
- فعّل المصادقة الثنائية لجميع حساباتك.

إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هو التنمّر الإلكتروني؟

هو إساءة أو مضايقة متعمّدة تتم عبر الوسائل الرقمية مثل الرسائل المسيئة، السخرية، نشر الشائعات، أو مشاركة صور بهدف الإيذاء، وقد تحدث عبر مواقع التواصل أو الرسائل أو الألعاب الإلكترونية.

كيف تحمي نفسك؟

- لا تتفاعل مع الرسائل المسيئة.
- اضبط الخصوصية لمنع الغرباء من التواصل.
- احظر المتنمّر فوراً من جميع المنصات.
- لا تشارك معلومات يمكن استغلالها ضدك.

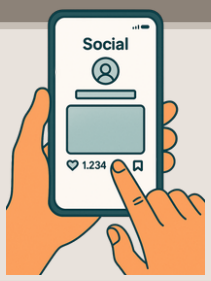
إذا وقعتَ ضحية للجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هو اختراق الحسابات الشخصية؟

هو وصول غير مصرح به إلى حساباتك عبر سرقة كلمات المرور، أو صفحات تسجيل دخول مزيفة، أو برمجيات خبيثة، أو مشاركة رمز التحقق مع شخص ينتحل الثقة.



كيف تحمي نفسك؟

- استخدم كلمات مرور قوية ومختلفة لكل حساب.
- فعّل خاصية المصادقة الثنائية.
- لا تضغط على أي رابط مجهول.
- سجّل الدخول دائماً من التطبيق أو الموقع الرسمي.
- راقب سجلّات الدخول بشكل دوري.

إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هي البرمجيات الخبيثة؟

هي برامج ضارة تُستخدم لاختراق الأجهزة أو إتلاف البيانات أو سرقتها دون علم المستخدم.
قد تأتي على شكل ملفات مرفقة، تطبيقات مزيفة، أو روابط تحميل غير آمنة، وتشمل الفيروسات وبرامج التجسس والفدية وغيرها.

كيف تحمي نفسك؟

- لا تفتح أي ملف مجهول المصدر.
- تجنّب تثبيت التطبيقات من مصادر غير رسمية.
- استخدم برنامج حماية موثوق وحدّثه باستمرار.
- لا تثبّت أي برنامج مكسور أو معدل.
- حدّث نظام التشغيل والتطبيقات بشكل دوري.

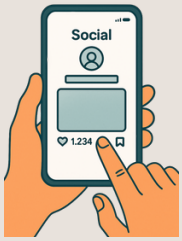
إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هو انتحال الشخصية؟

هو إنشاء هوية مزيفة أو استخدام هوية شخص آخر لخداع الضحية لطلب المال أو الوصول لمعلومات. قد يتم عبر رسائل أو اتصالات باستخدام اسم أو صورة مشابهة لاستغلال ثقة الضحية.



كيف تحمي نفسك؟

- تأكد من هوية صاحب الحساب قبل الرد أو التحويل.
- تجنب الضغط على الروابط من حسابات جديدة أو غريبة.
- راجع اسم المستخدم وتاريخ إنشاء الحساب للتأكد من المصداقية.
- تواصل مع الشخص الحقيقي عبر رقم معروف للتحقق من صحة الطلب.

إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعياً
BE AWARE

شرطة الشارقة
Sharjah Police

ما هي المواقع المزيّفة؟

هي مواقع تبدو حقيقية لكنها تهدف للاحتيال، مثل بيع منتجات غير موجودة أو سرقة بيانات الدفع، وغالباً تظهر عبر إعلانات مريبة أو تستخدم أسماء شبيهة لمتاجر معروفة لجذب الضحية.

كيف تحمي نفسك؟

- لا تشترِ من مواقع تصل عبر إعلان غير رسمي.
- تأكّد من عنوان الموقع وتجنّب الأسماء الغريبة.
- تأكّد من وجود وسائل دفع آمنة.
- لا تدخل بياناتك البنكية في مواقع غير معروفة.
- استخدم المواقع الرسمية والتطبيقات المعتمدة فقط.

إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

ما هو التزييف العميق (Deepfake)؟

هو تعديل الصور أو الفيديو باستخدام الذكاء الاصطناعي لإنشاء محتوى يبدو حقيقيًا لكنه مُفبرك بالكامل. يُستخدم للتضليل أو الابتزاز عبر إظهار الشخص في موقف لم يحدث.

كيف تحمي نفسك؟

- لا تثق بأي مقطع من مصدر مجهول.
- تحقق من مصدر المحتوى قبل مشاركته أو الرد عليه.
- تجنّب إرسال صور أو فيديوهات شخصية.
- راقب الحسابات التي تستخدم صورتك أو هويتك بشكل غير طبيعي.

إذا وقعتَ ضحية لجريمة، فأبلغ فوراً عبر الاتصال على 901 أو من خلال خدمة نجيد.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Is Cyber Extortion?

It is a form of threat delivered through any digital platform to force you to pay money or carry out certain requests using real or fabricated photos or personal information.
It often starts casually, then turns into a direct threat.

How Can You Protect Yourself?

- Do not share personal photos or information online.
- Adjust your privacy settings on all accounts.
- Avoid unknown links and attachments.
- Use strong and unique passwords for every account.
- Do not trust anyone requesting personal content.

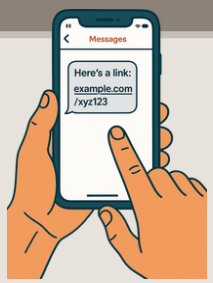
If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Is Phishing?

It is a scam that tricks victims into revealing sensitive information through messages or links that appear legitimate.
Attackers convince the victim to click and enter their data on a fake page.
It can occur through emails, texts, social media, or QR codes.



How Can You Protect Yourself?

- Do not open links from unknown or unofficial sources.
- Verify the link before clicking, and avoid shortened links.
- Access sensitive services (like banks) only through official apps.
- Enable two-factor authentication on all accounts.

If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Is Cyberbullying?

It is intentional harassment or repeated bullying through digital platforms, such as offensive messages, mocking content, spreading rumors, or sharing private information to cause harm. It may occur on social media, messaging apps, or online games.

How Can You Protect Yourself?

- Do not engage with harmful messages.
- Adjust privacy settings to block strangers.
- Block the bully on all platforms.
- Do not share information that could be misused.

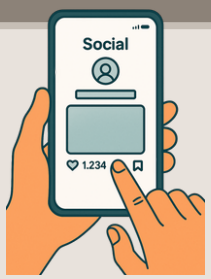
If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Is Account Hacking?

It is unauthorized access to your accounts through stolen passwords, fake login pages, malware, or sharing verification codes with someone pretending to be legitimate.



How Can You Protect Yourself?

- Use strong, unique passwords.
- Enable two-factor authentication.
- Avoid unknown links.
- Log in only through official apps.
- Check your login activity regularly.

If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Are Malware?

Malware are harmful programs that infiltrate devices, damage data, or steal information without the user's knowledge.
They often come through infected files, fake software, or malicious links and include viruses, spyware, ransomware, and trojans.

How Can You Protect Yourself?

- Do not open files from unknown sources.
- Avoid installing apps from unofficial websites.
- Use a trusted antivirus and keep it updated.
- Do not install pirated or modified software.
- Update your system and apps regularly.

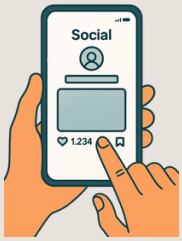
If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Is Identity Impersonation?

It is when someone creates a fake identity or uses another person's identity to deceive the victim into giving money or information. It is often done through messages or calls using similar names or photos to gain trust.



How Can You Protect Yourself?

- Confirm the person's identity before replying or sending money.
- Avoid clicking links from new or unfamiliar accounts.
- Check the username and account creation date to verify authenticity.
- Contact the real person directly using a known number to confirm the request

If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Are Fake Websites?

They are fraudulent sites designed to look real, used to trick victims into buying fake products or stealing payment information. They often appear through suspicious ads or use names similar to known stores.

How Can You Protect Yourself?

- Do not buy from websites reached through unofficial ads.
- Check the website URL and avoid strange or unfamiliar names.
- Verify that secure payment methods are available.
- Avoid entering your banking information on unknown sites.
- Use official and trusted apps/websites only.

If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.

كن واعيا
BE AWARE

شرطة الشارقة
Sharjah Police

What Is Deepfake?

It is the use of AI to alter images or videos to create realistic but fully fabricated content. It is used to mislead or blackmail by showing someone in a scenario that never happened.

How Can You Protect Yourself?

- Do not trust videos or images from unknown sources.
- Verify the origin before responding or sharing.
- Avoid sending personal photos or videos.
- Watch for accounts using your image or identity unusually.

If you become a victim of the crime, report it immediately by calling 901 or through the Najeed service.