CMRPI

المركز المغربي للأبحاث
المتعددة التقنيات و الابتكار

Financé
par l'Union européenne
et le Conseil de l'Europe

UNION EUROPÉENNE

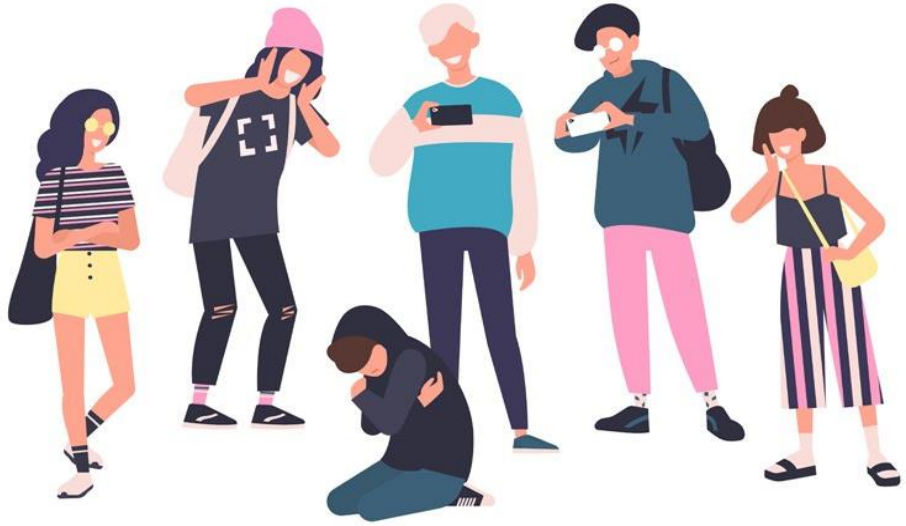
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Mis en œuvre
par le Conseil de l'Europe

المملكة المغربية
وزارة الشباب والثقافة والتواصل

Royaume du Maroc
Ministère de la Jeunesse, de la Culture et de la Communication



ورشات تدريبية نموذجية

قطاع الشباب - جهة الدار البيضاء سطات

تكوين فرق الموارد المتخصصة في التعامل مع حالات العنف السيبراني التحرش الإلكتروني في وسط الشباب

بوزنيقة ، فبراير 2023

سيرة ذاتية مختصرة :

- **أستاذ باحث في الرياضيات و الإعلاميات،** جامعة ابن طفيل ، القنيطرة ، المغرب.
- **الرئيس المؤسس للمركز المغربي للأبحاث المتعددة التقنيات و الابتكار CMRPI** www.cmrpi . (منذ 2012).
- **خبير مجلس أوروبا** في الأمن السيبراني وحماية الأطفال في البيئة الرقمية
- **مدير الحملة الوطنية لمكافحة الجرائم الإلكترونية في المغرب** - CNLCC 2014-2017
- **منسق اللجنة الوطنية لليوم العالمي لإنترنت أكثر أمنا بالمغرب،** منذ 2018.
- **مدير فضاء مغرب الثقة السيبرانية Espace Maroc** Cyberconfiance **www.cyberconfiance.ma منذ** 2020
- **منتدب قضائي من الدرجة الثانية سابقا** بالإدارة المركزية لوزارة العدل (خبرة 10 سنوات).

وحدة 1

العنف السيبراني ، مخاطر الإنترنت ، الجوانب التقنية

الفصل 1

الجوانب التقنية للجرائم الإلكترونية عند الأطفال والشباب

الإنترنت رائع ، لكن وجب الحذر!

الإنترنت عالم رائع للجميع! يمنح الكثير من الفرص ول عدة مزايا :

- وسائل الاتصال و التواصل
- وسيلة للتعلم
- وسيلة للترفيه
- وسيلة للتطور و الارتقاء
- إلخ

لقد أظهرت أزمة كوفيد بالملموس أهمية الإنترنت.

على الرغم من المزايا العديدة للإنترنت ،
يضم أيضا مخاطر محتملة! تتمثل في الأوجه العديدة للجرائم الإلكترونية

تقدر الخسائر البشرية والاقتصادية للجرائم العلوماتية بنحو **600 مليار دولار** ، أي 50 ضعف الناتج المحلي الإجمالي للمغرب ، أو ما يقرب من ضعف الناتج المحلي الإجمالي لفرنسا.
لقد أصبحت الجريمة الإلكترونية تحديا كبيرا و وحشًا.

على الرغم من المزايا العديدة للإنترنت إلا أنها تنطوي على مخاطر عديدة! وهي الجرائم الإلكترونية

في الوقت الحالي ، يستفيد مجرمو الإنترنت من إمكانيات الإنترنت: كتقنيات**إخفاء الهوية والتشفير** ، ولكن أيضًا التقنيات الجديدة ، لتنظيم أنفسهم بشكل أفضل ، لم يعودوا مجرد **قراصنة بسطاء (هواة)** ، لكنهم غالبًا ما يكونون **مجموعات منظمة جيدًا** . مجهزة بأحدث التقنيات.

تطور مخاطر الجرائم الإلكترونية

لسوء الحظ ، يتم استغلال جميع التطورات العلمية من قبل مجرمي الإنترنت.

بدون القدرة على التعرف عليهم ، يمكن لمجرمي الإنترنت الآن استخدام الذكاء الاصطناعي ، ولا سيما "التعلم الآلي" لاستغلال **الأطفال والشباب ، وبالتالي التلاعب بهم من خلال البرمجيات،**

لا يزال مستقبل الذكاء الاصطناعي يخفي مفاجآت للأمن على الإنترنت.

الجريمة السيبرانية معقدة للغاية : لليس من السهل السيطرة عليها

اليوم نحن نتحكم في أقل من 10٪ من محتوى الإنترنت

- **الإنترنت السطحي** (**Surface Web** / Surface Web)

تمثل حياتنا اليومية على الإنترنت ، من خلال رسائل البريد الإلكتروني ، التواصل عبر الشبكات الاجتماعية ، والتسوق عبر الإنترنت ، وما إلى ذلك. هذه المواقع فهي مفهرسة بواسطة محركات البحث.

- **الويب العميق** (**الويب المخفي Deep web**)

تقدر بنسبة 70 أو 75٪ من إجمالي الويب ، و ويشكل كل **المحتويات التي لم تتم فهرستها** بواسطة محركات البحث، و يتم الوصول إليها بواسطة برامج خاصة و أحيانا سرية.

- **الويب المظل** (**Dark web**)

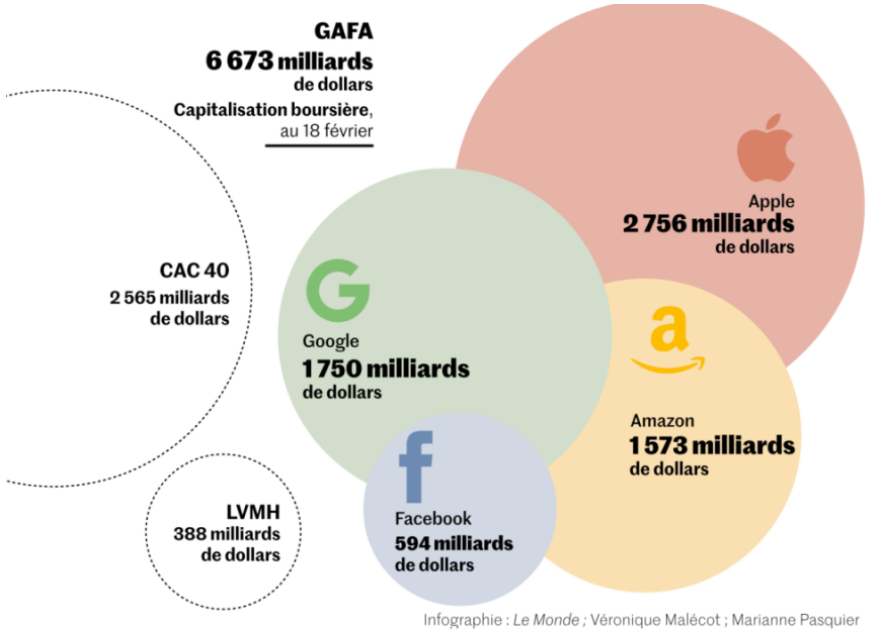
لا تصل إليها محركات البحث: بيع البطاقات البنكية ، والأسلحة، والمخدرات ، والتزوير ، **والمواد الإباحية للأطفال** ، وتوظيف القتلة ، ونقل الأعضاء البشرية، وشراء البرامج الضارة ، وما إلى ذلك.

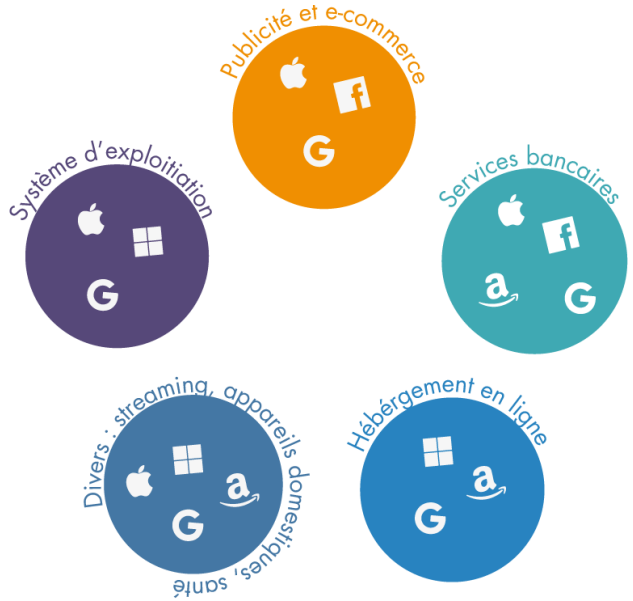
احتكار الإنترنت

يحتكر عمالقة الإنترنت نسبة 10٪ من شبكة الويب السطحية التي نتحكم فيها اليوم ، وبالتحديد GAFAM:

جوجل ، آبل ، فيسبوك (ميتا) ، أمازون ، مايكروسوفت ، بالإضافة إلى BATX العملاق الرقمي الصيني الناشئ

عمالقة الإنترنت هم قوة اقتصادية تكنولوجية ، يمكنهم حتى التأثير على السياسات





التحكم في حركة مرور معطيات الويب ومراقبتها وكذلك امتلاك البنية التحتية الخاصة

- حوالي **95٪** من الكابلات البحرية للألياف البصرية تربط القارات؛
- حوالي **80٪** من بيانات العالم مخزنة في مراكز البيانات الأمريكية في وادي السيليكون ، كاليفورنيا

الأمن السيبراني والحماية عبر الإنترنت / ضرورة التعاون مع عمالقة الإنترنت

يجب أن تخضع أي استراتيجية للأمن السيبراني والحماية عبر الإنترنت بشكل حتمي للتعاون مع عمالقة الإنترنت

"من يملك المعلومة يملك القوة ومن يتمكن من معالجتها يمسك العالم "

مقولة للفيلسوف آدام سميرس

عمالقة الإنترنت يخزنون المعلومات (مراكز البيانات)

المعالجة (تحليل البيانات ، البيانات الضخمة)

.

محاربة الجريمة السيبرانية: أبعاد متعددة

- **الجانب التقني**
تأمين البنية التحتية والمعدات

- **الجانب القانوني**
النصوص القانونية المتطورة والمحدثة

- **الجانب التنظيمي**
مؤسسات متخصصة وفعالة على أرض الواقع

ولكن قبل كل شيء أيضًا الوعي بالمخاطر والممارسات الجيدة للاستخدام الآمن للإنترنت ، فإن جزءًا كبيرًا من هجمات المجرمين الإلكترونيين هو أصل راجع إلى الأخطاء البشرية.

حماية الأطفال والشباب على الإنترنت

يتعرض الأطفال والشباب اليوم، مثلهم مثل البالغين ، للعديد من أنواع الجرائم الإلكترونية ، مع درجة أكبر من المخاطر نظرًا لما يلي:

1. **هشاشة هذه الفئة**
2. **التواجد المستمر في الفضاء الرقمي**

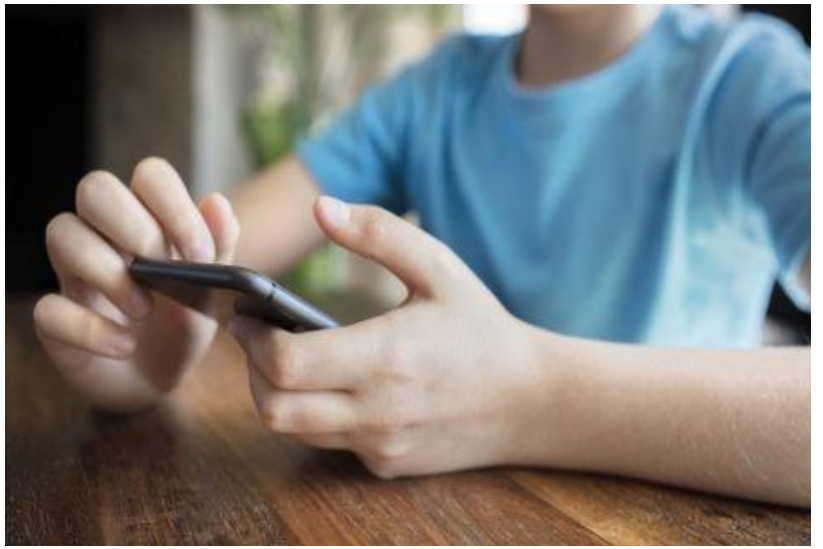
وهو ما يعقد مهمة حمايتهم على الإنترنت.

حماية الأطفال والشباب على الإنترنت

يحتاج الشباب، وخاصة الأطفال على الإنترنت ، إلى:

- **حماية خاصة وملائمة على الإنترنت**
- **مرافقتهم من أجل تعلم كيفية تجنب المخاطر**
- **معالجة خاصة إذا كانوا ضحايا وحتى فاعلين للجرائم الإلكترونية.**

حماية الأطفال والشباب على الإنترنت



- تتمثل حماية الأطفال على الإنترنت أولا في **فهم الجوانب التقنية والسلوكية المختلفة التي تمثل خطرًا أو تهديدًا عليهم** في البيئة الرقمية.
- الأخذ بعين الاعتبار **المخاطر الناشئة (عبر الذكاء الاصطناعي على سبيل المثال ، مما يجعل من الممكن تحليل سلوك الأطفال والشباب عبر الإنترنت** ، من خلال استغلال بياناتهم الشخصية)

تصنيف المخاطر الرقمية لدى الأطفال والشباب

- من أجل التبسيط ، يمكننا أن نستند إلى المبادئ التوجيهية للاتحاد الدولي للاتصالات ITU ، (2020) ، بشأن حماية الأطفال عبر الإنترنت
- يمكن تصنيف المخاطر الرقمية التي يلجأ إليها الأطفال عبر الإنترنت:

✓ **الفئة 1: المحتوى والتعامل**
✓ **الفئة 2: الاتصال بالبالغين أو الأطفال الآخرين**
✓ **الفئة 3: البرمجيات والأجهزة**

أهم أوجه العنف السيبراني لدى الأطفال والشباب

التعرض **لمحتوى غير لائق منشور على الإنترنت** أو **عنيف** أو **إباحي أو عنصري** أو محتوى **بغيض**
(يمكن أن يكون الطفل **ضحية أو فاعلا**)

أهم أوجه العنف السيبراني لدى الأطفال والشباب

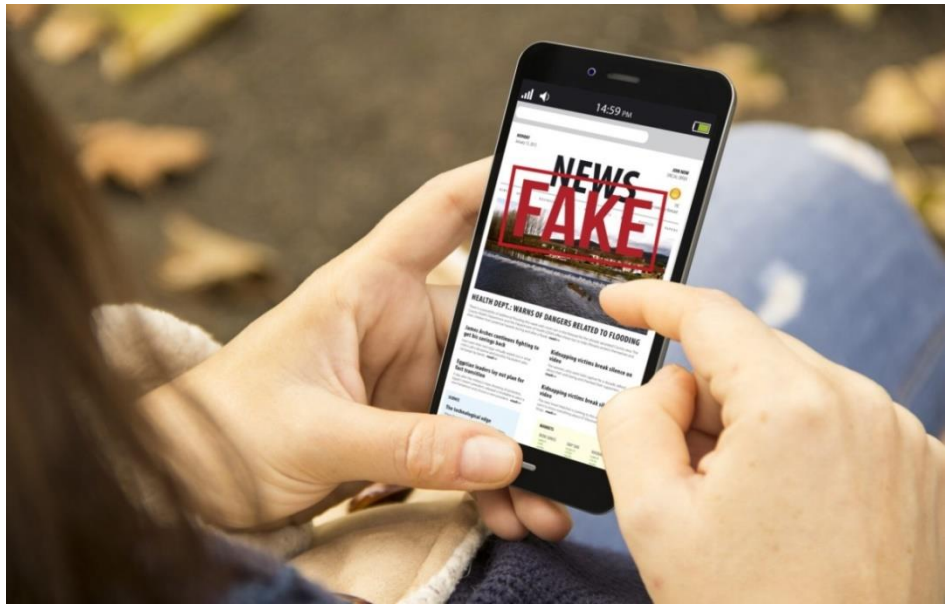
أفعال **التحرش والاستغلال الجنسي عبر الإنترنت** (نشر صور أو مقاطع فيديو حميمة) ، لأسباب متعددة: منها عنصرية أو دينية أو حتى توسيع نطاق الضرر الناجم في الحياة الواقعية إلى الحياة الافتراضية.

عواقب

الحزن ، الوحدة ، الأرق ، فقدان الثقة بالنفس ، التغيب عن المدرسة ... في بعض الأحيان ال يمكن أن تؤدي إلى الاكتئاب أو الانتحار .

الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال والشباب

التعرض **لمعلومات خاطئة** أو **معلومات** خاطئة أو معلومات غير دقيقة أو غير كاملة



عواقب

قد تتكون لدى الأطفال والشباب **نظرة مشوهة عن العالم** .

الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال والشباب

- **الاستمالة :** التلاعب النفسي من قبل شخص بالغ لأغراض جنسية ، **وبناء علاقة حميمة وعاطفية مع قاصر** .
- إنها ممارسة جديدة يتم إجراؤها من خلال **الشبكات الاجتماعية ومنتديات الدردشة ومواقع الألعاب على الانترنت**، من أجل الحصول على أفعال جنسيةمع طفل أوشباب (عبر كاميرا ويب على سبيل المثال) أو مقابلته في العالم الواقعي للإساءة إليه جنسيًا.
- من أجل كسب ثقة ضحيته بشكل أفضل، يتظاهر مجرم الإنترنت **بأنه طفل.**

الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال والشباب

ارسال الرسائل النصية : من خلال كلمات أو صور أو مقاطع فيديو جنسية صريحة مرسلة عن طريق الرسائل القصيرة (نتحدث أيضًا عن إرسال الرسائل الجنسية) أو تطبيقات الدردشة و المراسلات الفورية.

وهو نشاط يمارسه المراهقون بشكل رئيسي ؛

هناك نوعان مميزان:

- **إرسال الرسائل النصية الأولي**

عندما يبث شخص ما محتوى أو مقطع فيديو أو صورة حميمية أو خاصة إلى شخص آخر.

- **إرسال الرسائل النصية الثانوي :**

عندما ينقل فرد ما محتوى أو مقطع فيديو أو صورة حميمية لشخص ما نحو شخص ثالث أو أشخاص آخرين.

الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال والشباب

- **الابتزاز الجنسي الالكتروني** : ابتزاز عبر **كاميرا الويب** ، عندما يتم تهدد شخص ما بمشاركة صورة حميمة أو مقطع فيديو.

حاليًا ، شكل جديد من أشكال الابتزاز:

- باستخدام برامج تحرير الصور ، يضع مجرم الإنترنت وجوه الشباب أو الأطفال على مقاطع فيديو أو صور ليبدو أنهم عراة أو متورطون في أفعال جنسية، و بمنه يتم ابتزازاهم.

الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال والشباب

القذف والإضرار بالسمعة

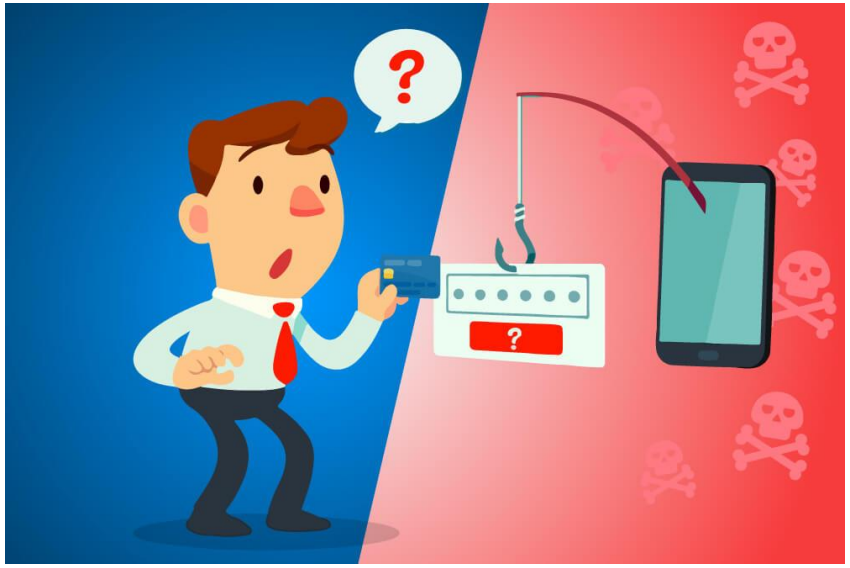
عندما ينشر شخص ما **على الإنترنت معلومات أو محتويات حول طرف ثالث** مع علمه بأنها خاطئة (أو حتى صحيحة) ، بقصد الإيذاء وتشويه السمعة.

الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال والشباب

سرقة الهوية

- يقصد به استخدام المعلومات الشخصية لشخص دون موافقته للقيام بأعمال احتيالية.
- من الناحية العملية ، يمكن لمجرمي الإنترنت الحصول على هذه المعلومات من خلال رسالة تصيد ، أو **اختراق أحد** الحسابات أو الأجهزة عبر الإنترنت ، أو حتى عن طريق **اختراق موقع ويب** تم فيه تخزين هذه المعلومات عليه.

سرقة البيانات عن طريق تقنيات التصيد



التصيد الاحتيالي

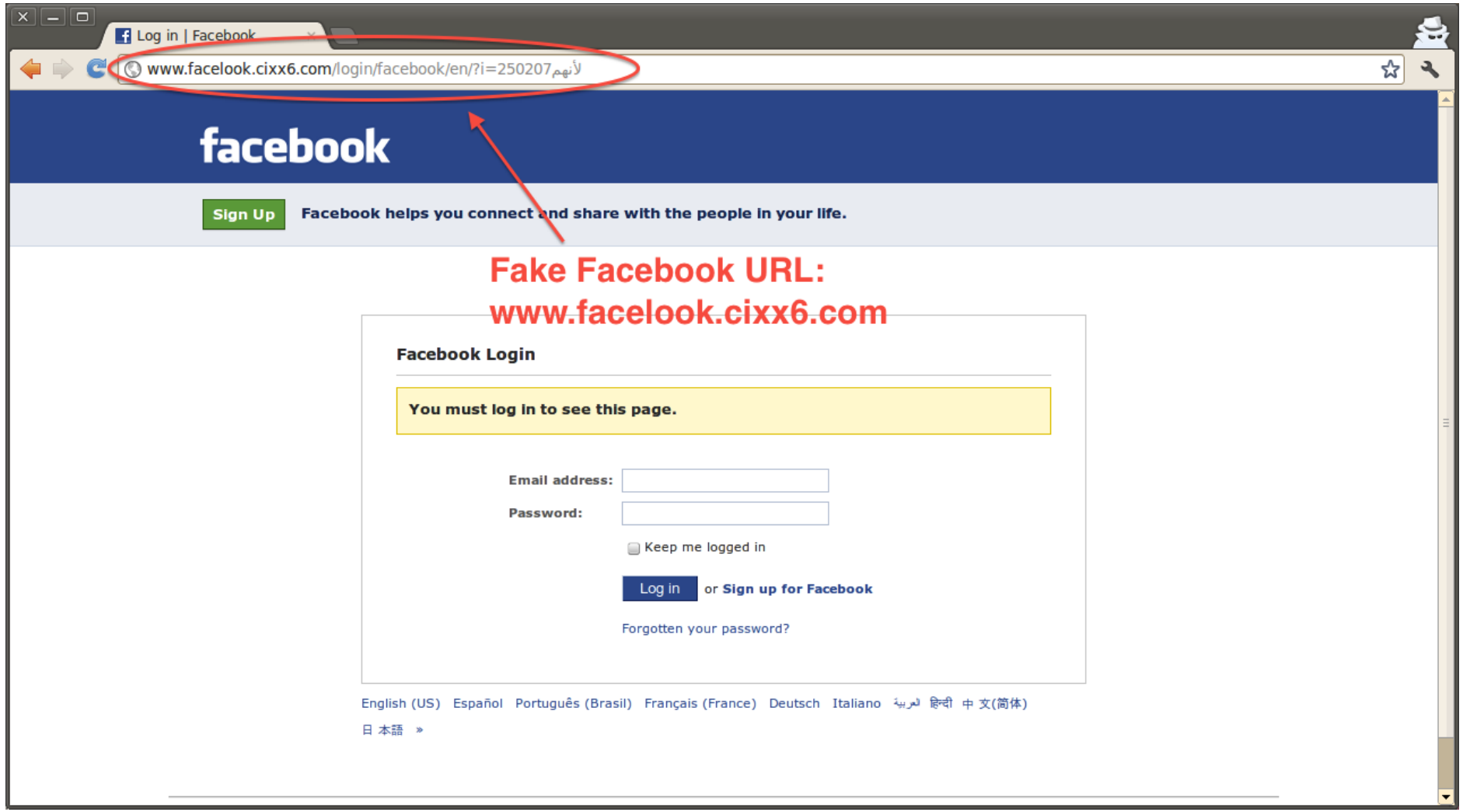
تقنية اختراق البيانات (الاحتيال) التي تهدف إلى استعادة المعلومات الشخصية ، من خلال تشجيع الأطفال على للبوح بكلمات المرور الخاصة بهم.

سرقة البيانات عن طريق تقنيات التصيد

كيف يتم ذلك (مثال)؟

1- يقوم المخترق بإجراء بحث بسيط على الإنترنت عن عنوان البريد الإلكتروني للضحية.
2- يقوم بإرسال بريد إلكتروني إلى الهدف، يطلب منه على سبيل المثال تحديث معلوماته على منصة ما، لأسباب تتعلق بالصيانة التقنية للتطبيق أو لأسباب تتعلق بترحيل الخادم.
3- يتم توجيه الضحية إلى صفحة ويب مزيفة **تشبه إلى حد بعيد الصفحة الأصلية ومن يتم يطلب منه** إدخال اسم المستخدم وكلمة المرور.
4- ومن تم يقوم المجرم الإلكتروني باستعادة كلمة المرور وتغييرها بسرعة.

سرقة البيانات عن طريق تقنيات التصيد



(عنوان URL: عنوان صفحة الويب غير متوافق)

احتيال وابتزاز كاميرا الويب

كيف يتم ذلك (مثال)؟

- يتم التوصل من متسلل مجهول أو يدعي أنه اخترق حساب بريدك الإلكتروني و أنه تمكن أيضا من اختراق إلى هاتفك الذكي وقد أطلع منذ فترة على نشاطك وزاراتك لمواقع مشبوهة

- ثم يهددك بنشر صور ومقاطع فيديو يدعي أنها إلتقطها لك خلسة من دون علمك بكاميرا الويب الخاصة بك ويطلب فدية بالعملة الافتراضية وإلا قام بنشرها على قائمة أصدقائك ومعارفك.

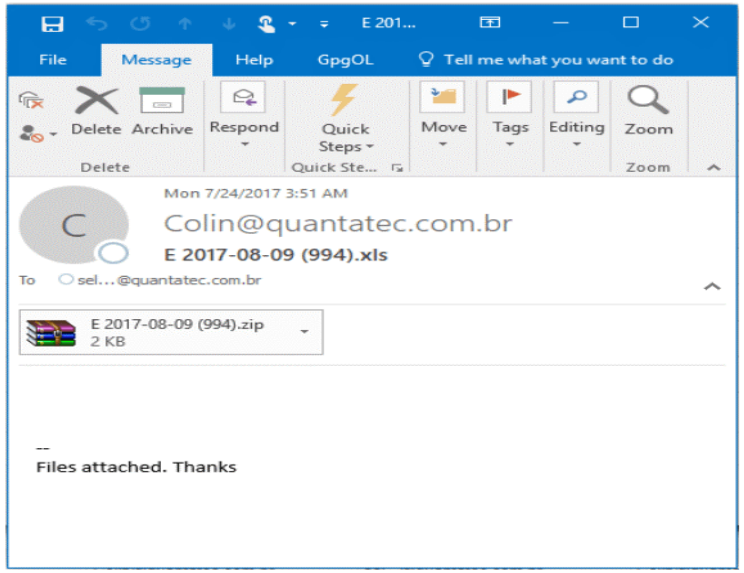
برامج الفدية وتشفير البيانات

برنامج الفدية الخبيثة ، وهو فيروس يقوم بتشفير ملفات الجهاز (أجهزة الكمبيوتر الشخصية ، والهواتف الذكية ، والأجهزة اللوحية ، والخوادم ، وما إلى ذلك)

يمكن أن ينتشر عبر الشبكة ويصيب سلسلة من الآلات.

بعد التشفير ، يقوم المخترق بإجبار الضحية على دفع فدية تتراوح من مئات إلى عدة آلاف من الدولارات ، على شكل عملة افتراضية (بيتكوين)

برامج الفدية وتشفير البيانات



كيف يتم ذلك (مثال)؟

عادةً ما يتلقى الضحية بريدًا إلكترونيًا يحتوي على مرفقات (ملف مضغوط أو صورة ، أو غيرها)

بعد تنزيل المرفقات وفتحها ، يصاب الجهاز بالفيروس ويتم تشفير الملفات.

يطلب المخترق فدية مع مهلة ما بين 24 إلى 48 ساعة، وإلا ستزداد الفدية.

هناك حالات لأطفال يقومون في مثل هذه الحالات من سرقة البطاقات المصرفية أو الأموال أو المجوهرات الخاصة بأوليائهم مثلا من أجل دفع الفدية.

نشرت البيانات الوصفية للصور مخاطرة كبيرة

خطر الصور المنشورة على الإنترنت

يمكن أن تحتوي الصور التي التقطتها الكاميرات الرقمية على الكثير من معلومات التعريف ، مثل **التاريخ** والوقت **والعلامة التجارية للكاميرا** التي تم **) لمكان GPS** التقاطها بها **وإحداثيات نظام تحديد المواقع العالمي (التقاطها** ، مما يشكل خطرًا كبيرًا على خصوصية الأطفال.

بدون معرفة ذلك ، يمكن للطفل أن يكشف للجميع أين يعيش ، من خلال نشر صورة بسيطة.

نشرت البيانات الوصفية للصور مخاطرة كبيرة

فيما يلي المعلومات الفنية المتعلقة بالبيانات الوصفية التي قد تحتوي عليها الصورة المنشورة على الإنترنت:

تعريف

احداثيات نظام تحديد الموقع

حقوق النشر

اسم الكاتب

عنوان

رقم الهاتف

البريد الإلكتروني

موقع إلكتروني

رخصة

البلد الذي تم التقاط الصورة فيه

آلة تصوير

العلامة التجارية والطراز

تاريخ اللقطة

سرعة مصراع الكاميرا

تعرض

فتحة الحجاب الحاجز

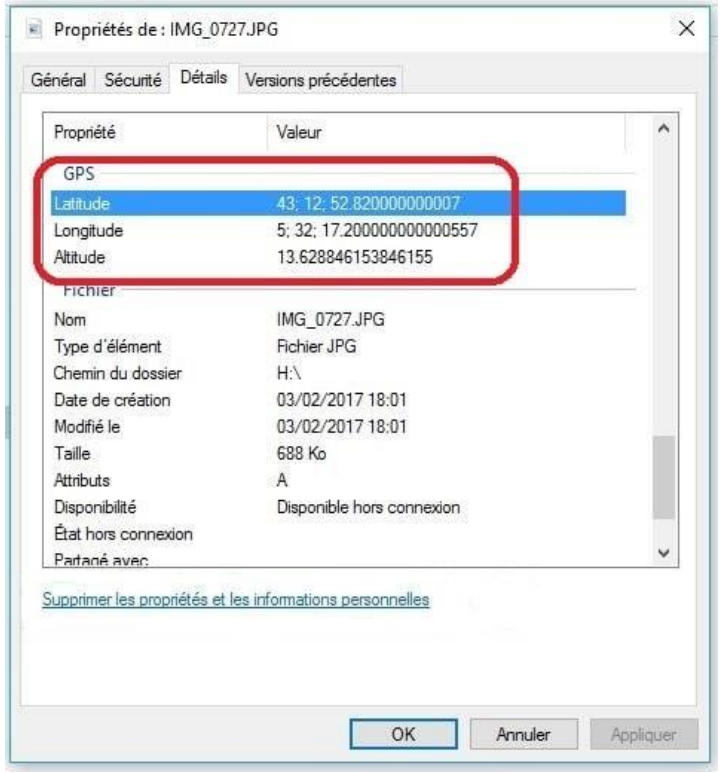
الحساسية (ISO)

المسافة البؤرية

موضوعي

وميض أو إيقاف تشغيله

مصدر ضوء



نشرت البيانات الوصفية للصور مخاطرة كبيرة

التصوير الرقمي هو أيضًا ناقل للهجوم الإلكتروني

من الممكن دائمًا إدخال **فيروس** في البيانات الوصفية للصورة ، وذلك بفضل البرامج المجانية مثل " Exiftool " (**برنامج يسمح بقراءة البيانات الوصفية للصورة وكتابتها ومعالجتها**)

يمكن بعد ذلك تنفيذ الكود (الفيروس) بمجرد تنزيله وبالتالي يقوم الفيروس ب (إتلاف الجهاز ، والتجسس ، والسيطرة ، وتنشيط الكاميرا والميكروفون عن بُعد)

يجب إزالة البيانات الوصفية من الصور قبل مشاركتها أو نشرها

ملفات تعريف الارتباط والتجسس Cookies

ملفات تعريف الارتباط (Cookies)هي برامج تستخدمها مواقع الويب لتتبع أنشطة الزائر وتفضيلاته لأغراض التسويق ، من حيث المبدأ لا تهدف هذه الممارسة إلى التجسس.

لكن من ناحية أخرى ، **يحاول المتسللون (القراصنة) الحصول على ملفات تعريف الارتباط** ، والهدف هو استغلال محتواها (معطيات شخصية، تفضيلات ...) واستخدام هذه البيانات الشخصية لأغراض ضارة.

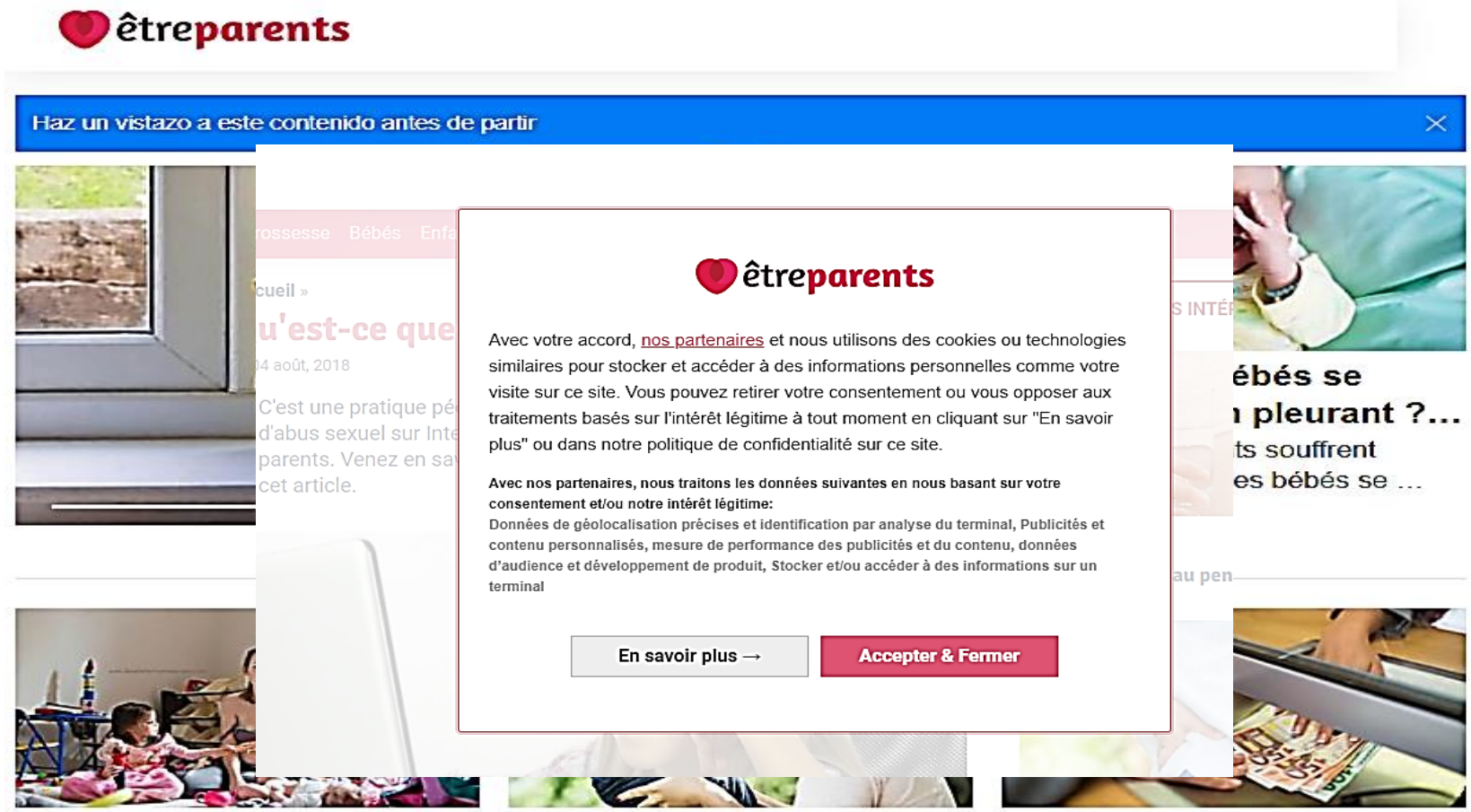
الجوانب الرئيسية للعنف عبر الإنترنت بين الأطفال

- **استغلال الأطفال من خلال الألعاب عبر الإنترنت** و التعرف على غرباء أو حتى بالغين **(دردشة ومجموعات النقاش)**
- **خطر محتمل للإدمان**

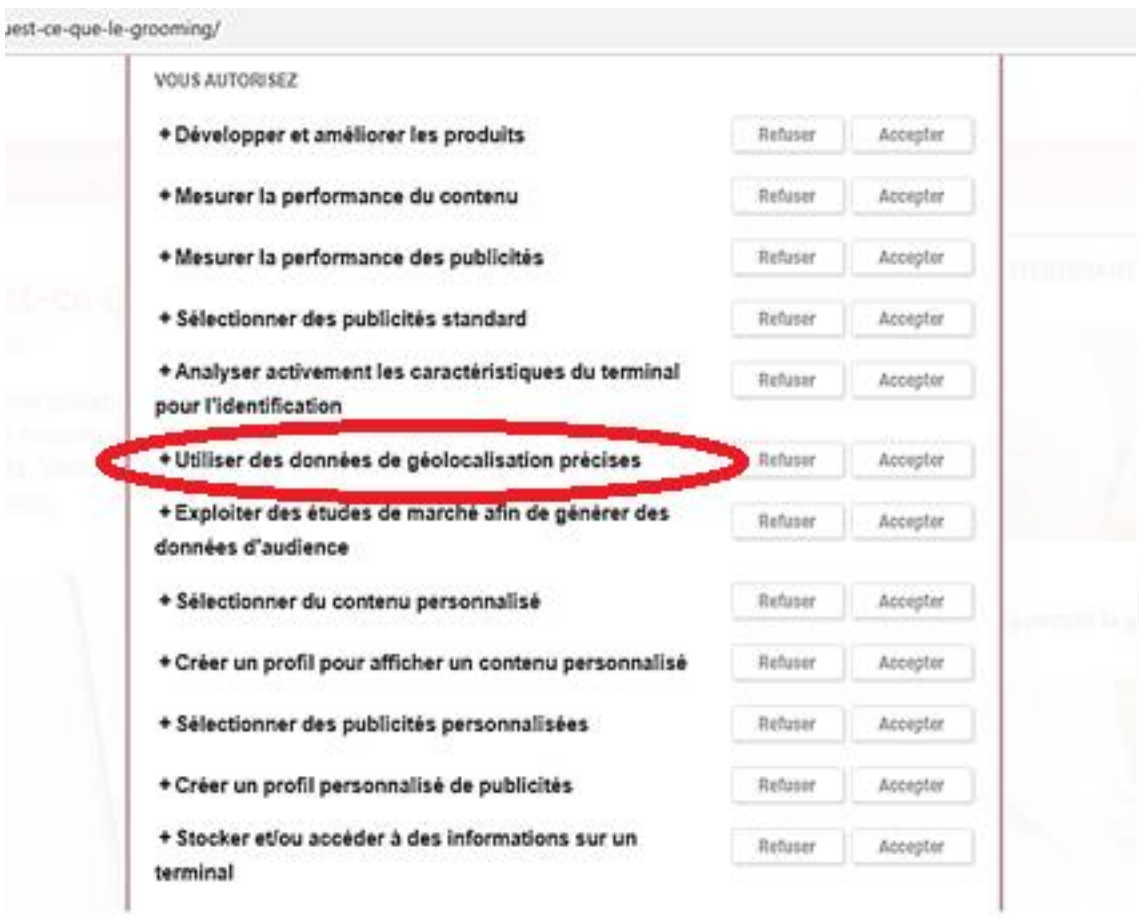
ملفات تعريف الارتباط والتجسس

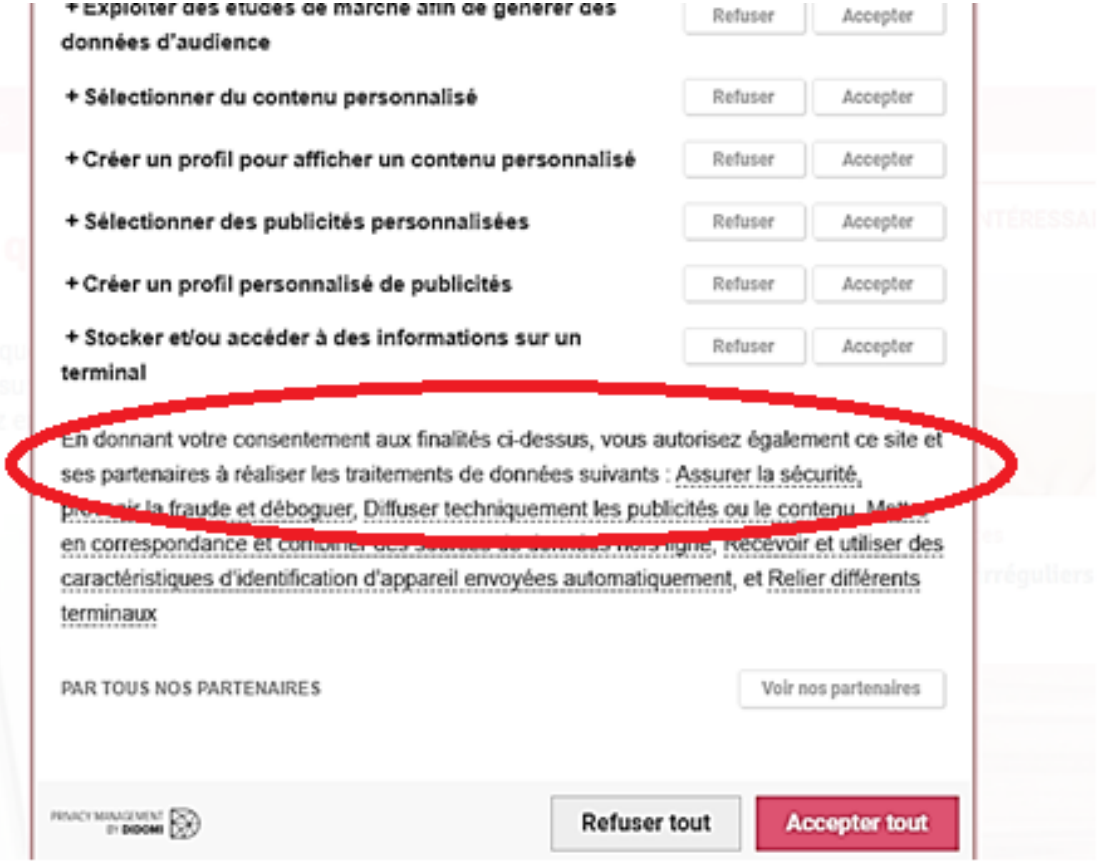
مثال :

https://etreparents.com/quest-ce-que-le-grooming/



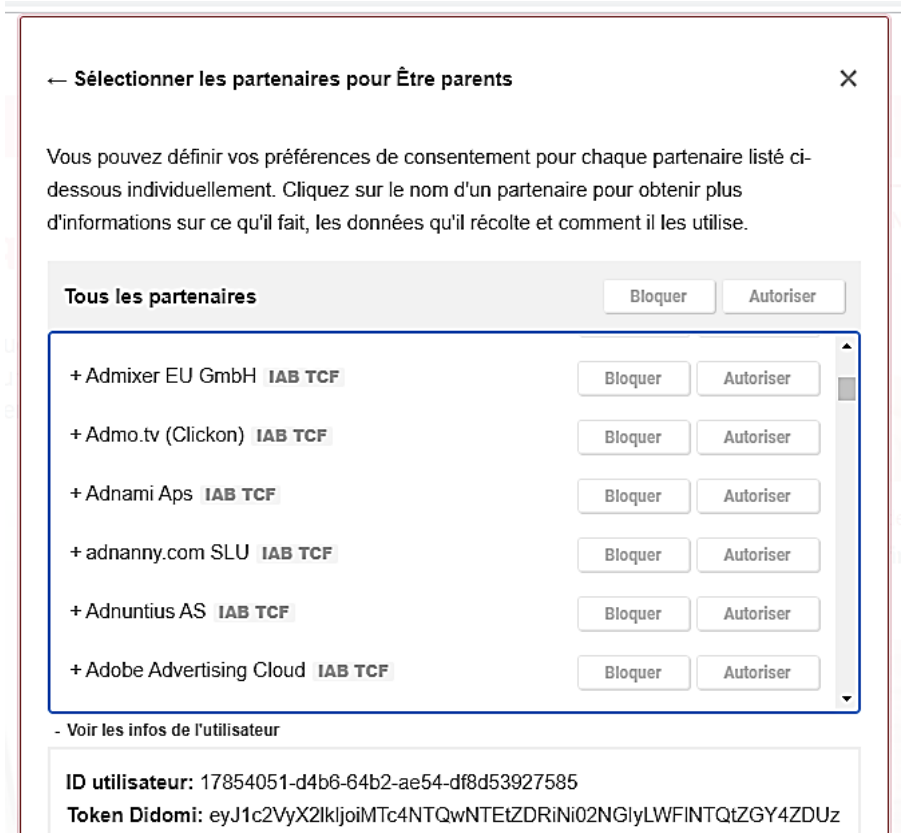
ملفات تعريف الارتباط والتجسس

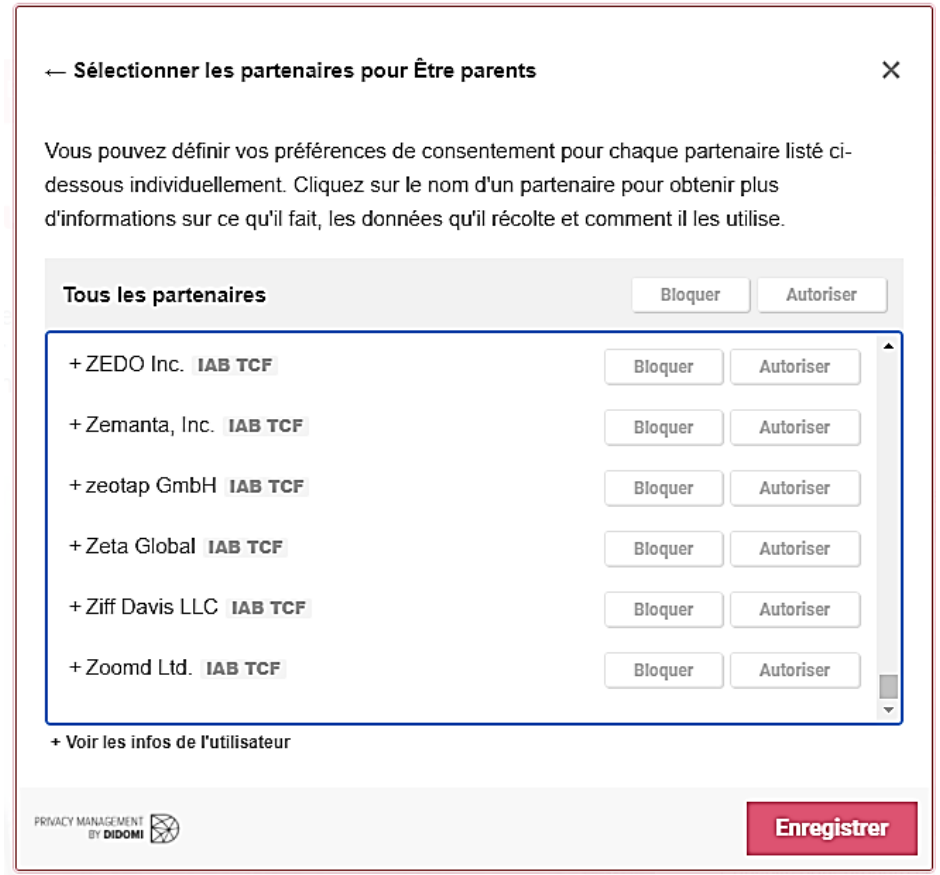




ملفات تعريف الارتباط والتجسس

تحتوي قائمة الشركاء على مائة على الأقل ، والتي تجمع البيانات الشخصية من زوار الموقع





ما رأيكم؟