الأمن الرقمي للمجموعات المدنية

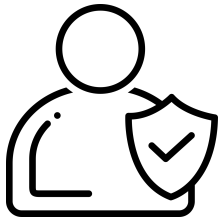
كيف ينطبق الأمن الرقمي عليك؟

خصوصية المعلومات

لا يتمكن الأشخاص غير المأذون لهم من الاطلاع على المعلومات، أو الوصول إليها، أو رؤيتها

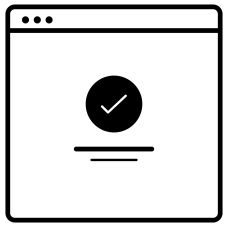
سلامة المعلومات

لا يتمكن الأشخاص غير المأذون لهم من تعديل المعلومات

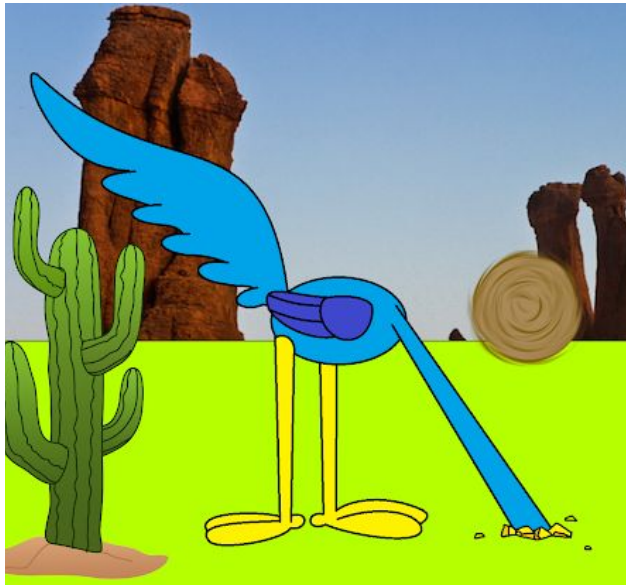


توفّر المعلومات

يمكن الوصول إلى المعلومات متى وأينما تدعو الحاجة إليها



المقاربات المشتركة نحو الأمن...



التي تُعتبر سيئة ...


...عوضاً عن ذلك، ما نريده هو
التفكير بشكل منطقي واستراتيجي

حماية حساباتك

تمرّن على إدارة كلمات السر بطريقة جيدة

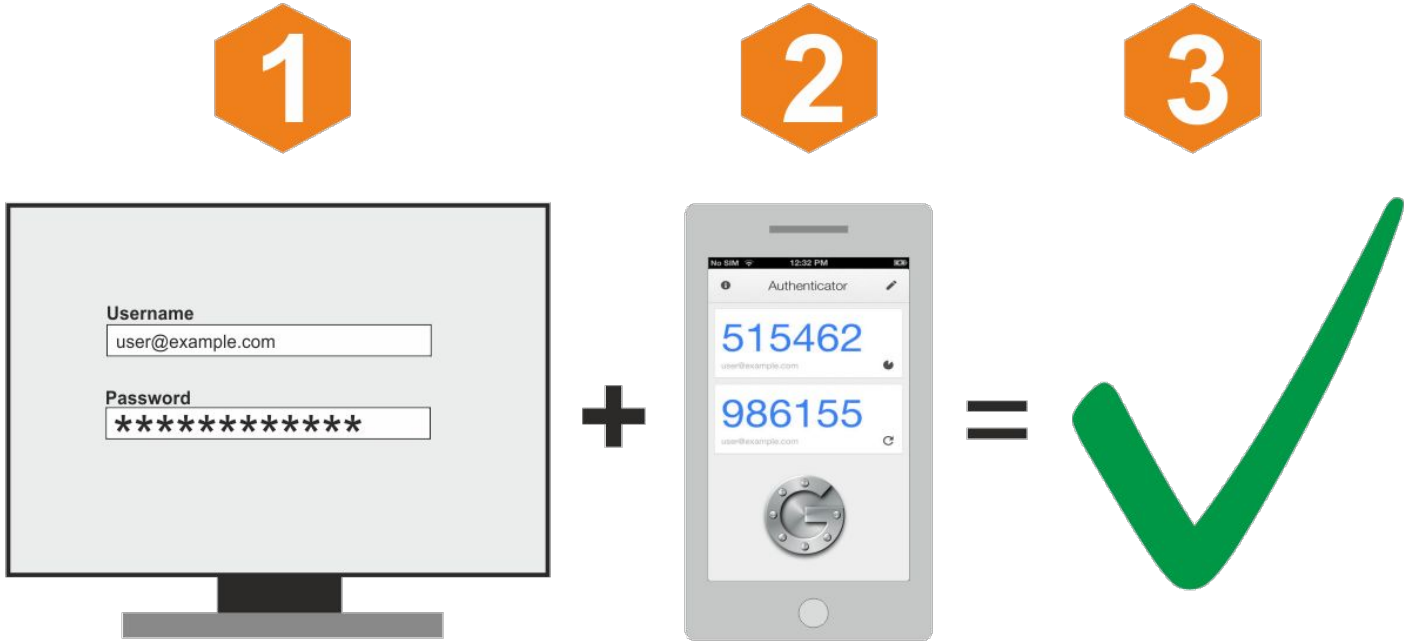
- استخدم كلمات سر **طويلة ومميّزة**
- من الأفضل اعتماد سلسلة من 3-4 كلمات عشوائية
- اعتمد **برنامجاً لإدارة كلمات السر**
- **تجنب الحسابات المشتركة** لكن بدّل كلمات السر عند الحاجة

Weak Passwords	Strong Passwords
L@1lip0p	lollipopcandlemustache
john2658	J93y572ohg0531nB1
asdfghk345678	MERj4t0q424EcHi57

استخدم برنامجاً لإدارة كلمات السر

طريقة لتخزين كلمات السر، واستردادها، وتوليد كلمات سر جديدة

استخدم خاصية التحقق بخطوتين



تنبّه من التصيد الاحتيالي

- التصيد الاحتيالي: هو عبارة عن رسالة وهمية (رسائل إلكترونية، نصية، عبر وسائل التواصل الاجتماعي) مصمّمة لحملك على:
  - النقر على رابط خبيث أو تنزيل ملف مرفق خطر
  - الإدلاء بكلمة السر الخاصة بك أو بمعلومات حساسة
- يمكن أن يؤدي إلى إصابة أجهزتك وتعريض حساباتك للخطر
- كيف يمكن تجنّب التصيد الاحتيالي؟
  - اطرح على نفسك بعض الأسئلة الأساسية مثل:
    - هل أتوقع تلقي هذه الرسالة الإلكترونية؟ هل عنوان البريد الإلكتروني هذا معروف بالنسبة إلي؟ هل يطابق "اسم" المرسل عنوان البريد الإلكتروني؟
  - مرّر المؤشر فوق الروابط الإلكترونية! هل تعرفت على الموقع الذي سينقلك إليه الرابط إذا نقرت عليه؟
  - احذر الملفات المرفقة، خاصةً ملفات .zip أو .exe

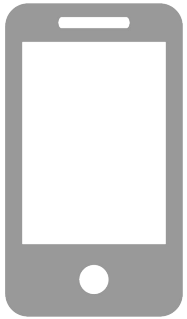
لا تقتصر تكتيكات التصيد الاحتيالي على رسائل البريد الإلكتروني فقط

التصيد الاحتيالي عبر وسائل التواصل الاجتماعي

(عبر حسابات احتيالية وتدوينات/مراسلات فورية خبيثة)

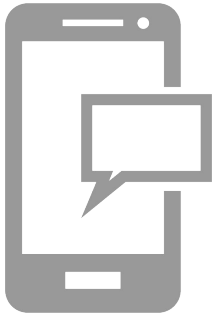
التصيد الاحتيالي عبر الرسائل الصوتية

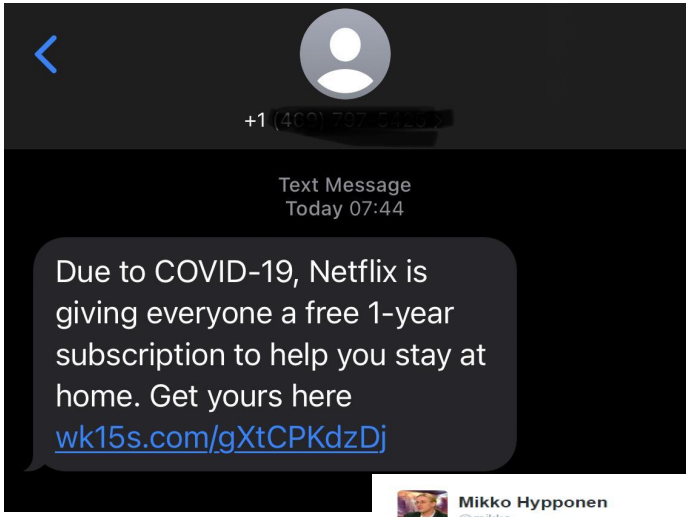
(يُعرف أيضاً بـ **"vishing"**)



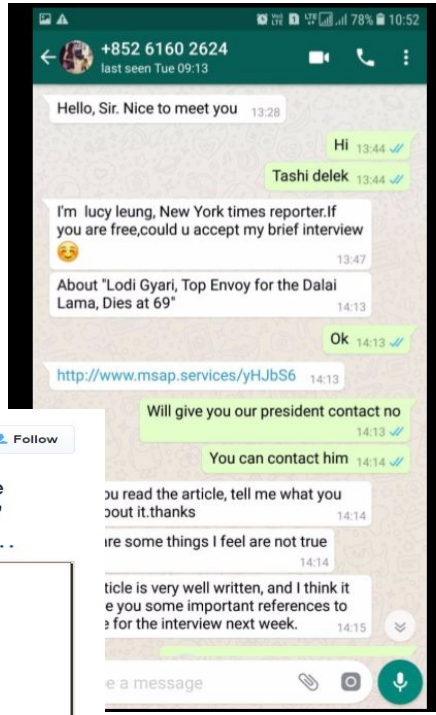
التصيد الاحتيالي عبر الرسائل النصية القصيرة

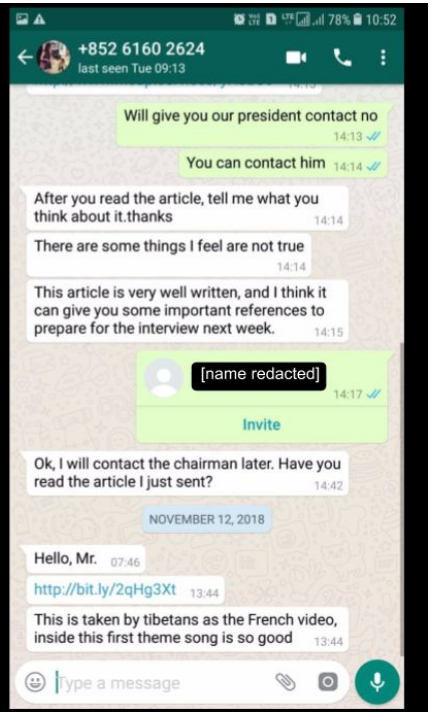
(يُعرف أيضاً بـ **"smishing"**)




+1 (469) 797-5445
Text Message
Today 07:44
Due to COVID-19, Netflix is giving everyone a free 1-year subscription to help you stay at home. Get yours here wk15s.com/gXtCPKdzDj


Mikko Hypponen
@mikko
Follow
This document, claiming to be from the @NDI, was used in the targeted 'Duke' attacks. See twitter.com/lehtior2/statu...
NDI
NATIONAL DEMOCRATIC INSTITUTE
Public Attitudes in Georgia
Results of a April 2015 survey carried out for NDI by CRRC Georgia
This research is funded by the Swedish International Development Cooperation Agency (Sida)
Laura Thornton - NDI Georgia
Davit Sichinava – CRRC Georgia
RETWEETS 11
FAVORITES 3
9:24 AM - 23 Jul 2015


+852 6160 2624
last seen Tue 09:13
Hello, Sir. Nice to meet you 13:28
Hi 13:44
Tashi delek 13:44
I'm lucy leung, New York times reporter.If you are free,could u accept my brief interview 13:47
About "Lodi Gyari, Top Envoy for the Dalai Lama, Dies at 69" 14:13
Ok 14:13
http://www.msap.services/yHJbS6 14:13
Will give you our president contact no 14:13
You can contact him 14:14
Type a message

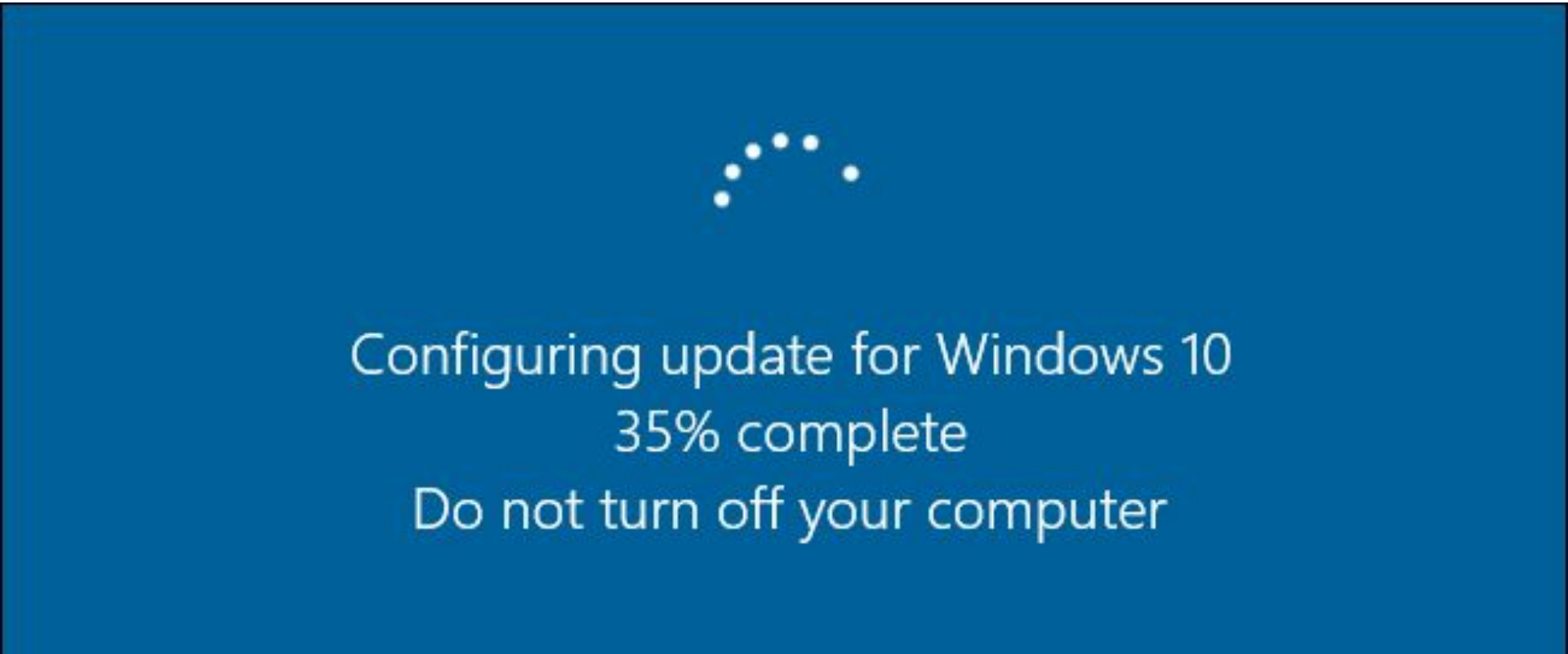

+852 6160 2624
last seen Tue 09:13
Will give you our president contact no 14:13
You can contact him 14:14
After you read the article, tell me what you think about it.thanks 14:14
There are some things I feel are not true 14:14
This article is very well written, and I think it can give you some important references to prepare for the interview next week. 14:15
[name redacted] 14:17
Invite
Ok, I will contact the chairman later. Have you read the article I just sent? 14:42
NOVEMBER 12, 2018
Hello, Mr. 07:46
http://bit.ly/2qHg3Xt 13:44
This is taken by tibetans as the French video, inside this first theme song is so good 13:44
Type a message

حماية أجهزتك

احتفظ بنسخة احتياطية عن بياناتك

حدّث أنظمتك باستمرار

(!الأمر أسهل بكثير إذا كنت تستخدم برنامج كمبيوتر شرعي)



استخدم برمجيات مضادة للفيروسات

تحكّم بما يدخل إلى شبكتك

تجنّب استخدام شاحن عام لمفاتيح الذاكرة (USB) وغير ذلك من الأجهزة "المشتركة"

(لكن إذا فعلت ذلك، فكّر في استخدام حاجب للبيانات يُستخدم مع مفاتيح الذاكرة)

تصفح المواقع بطريقة ذكية

حماية معلوماتك ورسائلك

استخدم المراسلة المشفرة

ماذا عن واتساب؟ إنه مشفر وفق نظام التشفير التام من طرف إلى آخر، لكن قد ينطوي فايسبوك على خطر تشارك البيانات.

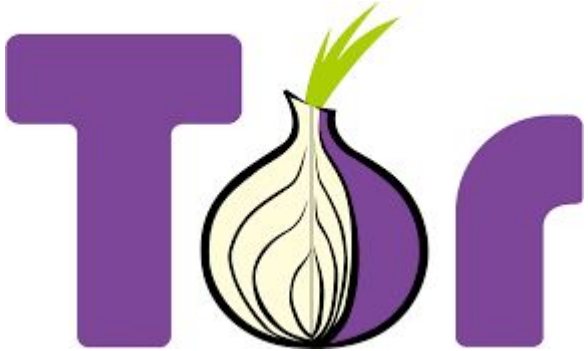
استخدم السحابة

استخدم أدوات للتصفح بشكل آمن

TunnelBear

privateinternetaccess

PSIPHON



مكافحة البوت والمتصيدين

بلّغ مزوّد الشبكة عن حسابات البوت المشبوهة

هل تقوم بالحظر، أو الإجابة، أو التجاهل؟

الجواب: يعتمد الأمر على الوضع

احمِ صفحتك: فايسبوك

تنبّه إلى إعدادات المشرف على الموقع!

- لا يمكنك تعطيل التعليقات على تدوينات صفحتك، ولكن يمكنك إخفاء تعليقات الأفراد أو حذفها
- أدر التعليقات والتدوينات التي ينشرها الزوار من خلال حظر كلمات معيّنة
- امنع بعض الأشخاص من زيارة صفحتك
- أوقف العمل بالمراجعات النقدية لصفحتك
- حدّد سياسة بشأن أنواع التعليقات المسموح بها على الصفحة

احمِ صفحتك: إنستاغرام

راجع إعدادات الخصوصية المتعلقة بك!

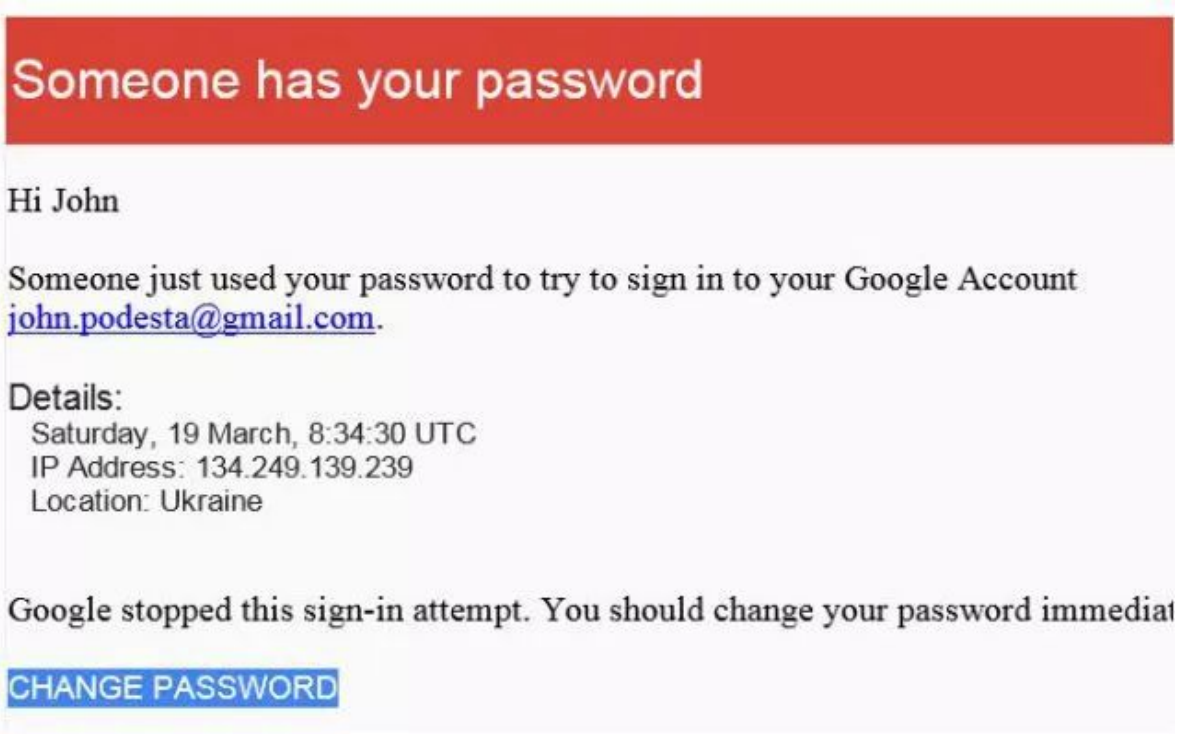
- احظر المستخدمين المسيئين للآخرين أو الذين ينشرون التعليقات المزعجة أو العشوائية، أو قم تقييدهم، أو الإبلاغ عنهم، أو منعهم من التعليق.
- أدر التعليقات غير المرغوب فيها
  - احذف كميات كبيرة منها في نقرة واحدة
  - شغل خاصية الإخفاء التلقائي للتعليقات المهينة
  - أوقف العمل بخاصية التعليقات
- تحكّم بمن يستطيع الإشارة إليك بوسم أو تعليق
- أوقف العمل بإمكانية التعليق على التدوينات

البشر: الحلقة الأضعف

صغ سياسات للأمن الرقمي وتدرّب عليها بانتظام

- يجب أن تكون التوصيات التي تختار الالتزام بها **مدمجة في السياسات**
- عند تعيين موظفين، **درّبهم** على هذه السياسات واطلب منهم التوقيع على الالتزام بها
- لا يتذكّر الأشخاص الأشياء إلى الأبد، كما أنّ أفضل الممارسات تتغيّر. لذا، **نظّم تدريبات لإنعاش ذاكرتهم** بانتظام

اطلب من جميع الموظفين/ المتطوعين/ المستشارين الالتزام بسياسات الأمن الرقمي



لا تنسَ الجوانب المادية

- قد تتضمّن الأوراق معلومات حساسة أيضاً، فخفف من استخدامها إلى الحد الأدنى وتخلص من المستندات السرية باستخدام آلة تمزيق الورق
- من المفيد استخدام أقفال الأبواب، وكاميرات المراقبة الأمنية، وحراس
- يمكن الوقاية من السرقة من خلال ربط أجهزة الكمبيوتر بالمكاتب عبر الكوابل

اعتمد إجراءات محددة لدى التحاق موظفين جدد بالخدمة/مغادرتهم

- عندما يغادر الأشخاص، غالباً ما يأخذون أشياء معهم، أو يعودون لأخذها لاحقاً
- امنع وصول الموظفين أو المتطوعين السابقين إلى الحسابات الرقمية في الحال- هل تعرف كل ما يمكنهم الوصول إليه؟
- هل تحتاج إلى تغيير أي قفل أوهل تعرف كيف تقطع عليهم أي طرق أخرى للوصول؟

كيف نصل إلى مكان أكثر أماناً؟

قم بإجراء تقييم شمولي لمخاطر المعلومات

من يريد النيل منك، وما هو مطلبهم؟

- ماذا يريد "الأشرار" من منظمتك؟

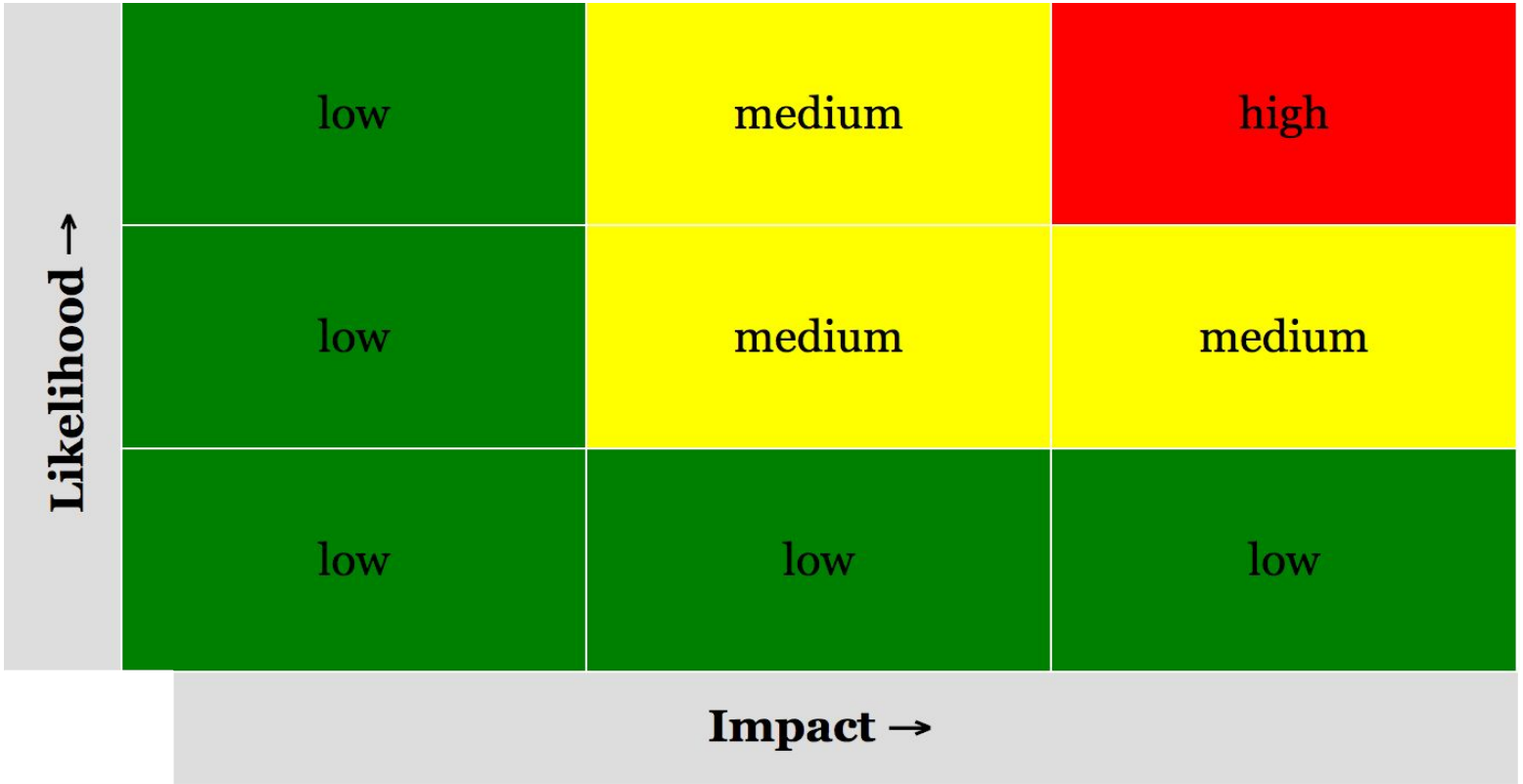
ما الذي يهمّك؟ ما هي أكبر أسرارك؟

- ما هي أكثر المعلومات التي تهمّك؟
- كي تنقل المعلومات وتصل إلى المعلومات التي تحتاج إليها؟

كيف تحدث الهجمات الرقمية اليوم؟

- ما هي أبرز الهجمات السيبرانية التي تحدث اليوم؟
- هل من هجمات خاصة ببلدك؟

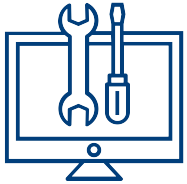
لا يمكنك القيام بكل شيء. أجر مسحاً للمخاطر ورتّبها بحسب الأولوية



إعداد خطط الاستجابة للطوارئ

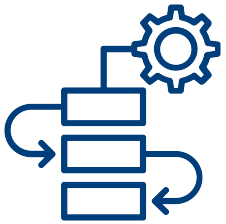
على المستوى القانوني

- افهم حقوقك القانونية في حال تعرّضت لهجمة سيبرانية
- وكّل محامياً
- كن ملماً بما هي واجبات الباعة تجاهك في حال تعرّضوا للقرصنة؛ احرص على وجود شروط للإبلاغ في العقود/الاتفاقات المبرمة معهم



على المستوى التقني

- حدّد نقطة اتصال تُعنى بالشؤون التقنية في منظمتك
- حدّد نقاط اتصال خارجية للحصول على الدعم التقني
- كن ملمّاً بنوع المساعدة التي يمكن لمزودي خدمة المنصة توفيرها لك في حال وقوع هجمة إلكترونية



العمليات

- كوّن فريقاً للاستجابة للحوادث
- حدّد تسلسل القيادة لتسريع عملية صنع القرار
- حدّد وسائل تكنولوجية بديلة للتواصل بين الموظفين إذا كنت تعتقد أنّ أنظمتك قد تعرضت للاختراق (مثلاً استخدم سيغنال عوضاً عن البريد الإلكتروني)

الاتصالات

- حدّد أصحاب المصلحة الذين يجب أن تتصل بهم في حال تعرّضت لحادث متعلق بالأمن الرقمي
- ضع خطة أو سيناريو يشرح كيفية التواصل في مختلف أنواع الحوادث السيبرانية، كما في الحالات التالية:
  - تمّ اختراق موقعك الإلكتروني/ حساباتك على مواقع التواصل الاجتماعي
  - تمّ اختراق البريد الإلكتروني لأحد الموظفين
  - تعرضت لعملية اقتحام فعلية، حيث تمت سرقة الخادم المحلي الذي يتضمّن كافة الملفات الإلكترونية للمنظمة

للمراجعة...

- صغ (ونفّذ) سياسات وإجراءات لحفظ الأمن
- خصص الموارد المطلوبة لتطبيق التوصيات، وشراء الأدوات، وتطبيق السياسات، وتدريب الموظفين
- راجع الإعدادات والأذونات الخاصة بحساباتك بانتظام
- صغ خططاً للاستجابة للحوادث
- لا تسمح لحفظ الأمن أن يكون فكرة ثانوية... بل ادمجه في كل ما تفعله!

موارد إضافية

- نحن، الفريق التقني في المعهد الديمقراطي الوطني (تويتر: @NDItech، بريد إلكتروني: nditech@ndi.org)
- هل تعرّضت كلمات السر الخاصة بك للقرصنة؟ https://haveibeenpwned.com/
- هل يمكنني استخدام خاصية التحقق بخطوتين على أنظمتي؟ https://twofactorauth.org/
- اخضع لاختبار حول التصيّد الاحتيالي! https://phishingquiz.withgoogle.com/
- قم بإجراء تقييم بسيط حول المخاطر الإلكترونية: https://securityplanner.org
- كتيّب الأمن السيبراني للحملات (www.belfercenter.org/cyberplaybook)
- الأمن في صندوق (https://securityinabox.org/)
- الأمن الشمولي من TacticalTech (https://holistic-security.tacticaltech.org/)
- خطة الاتصالات الخاصة بالحوادث السيبرانية (https://ndite.ch/cyberincidentcomms)