غرفة التجارة و الصناعة و الخدمات
لجهة طنجة - تطوان - الحسيمة
ⵜⴰⵅⵅⴰⵛⵜ ⵏ ⵜⵓⵙⵎⵎⴰⵙⵜ ⴰ ⵙⵓⵙⵏ ⴰ ⵜⵛⵍⴰⵀⵙⵜ
ⵜⴰⵛⵍⴰⵙⵜ ⵜⴰⵏⵔⴰ ⵜⵣⵜⵓⵔⴰⵏ ⵀⴰⵙⵓⵓⵣⵛⴰ
Chambre de Commerce d'Industrie et de Services
TANGER - TETOUAN - EL HOCEIMA

Bonnes Pratiques pour la Sensibilisation à la Cybersécurité

أفضل الممارسات للتوعية بالأمن السيبراني

2025

إصدارات الغرفة
أبريل 2025

C.C.I.S
TANGER-TÉTOUAN-AL HOCEIMA

Bonnes Pratiques pour la Sensibilisation à la Cybersécurité

أفضل الممارسات للتوعية بالأمن السيبراني

Introduction générale

Dans un contexte de transformation numérique rapide, la cybersécurité est devenue essentielle pour protéger les données et assurer la continuité des activités économiques et des services.

À travers ce guide, la Chambre de Commerce, d'Industrie et de Services de la région Tanger-Tétouan-Al Hoceima vise à sensibiliser ses membres et son personnel aux risques numériques et aux bonnes pratiques de sécurité.

Ce guide constitue un outil pratique de sensibilisation qui renforce la culture de la cybersécurité et fait du bon sens numérique un rempart fondamental contre les menaces électroniques, au service d'un environnement digital fiable et propice à l'investissement.

تقديم عام

في ظل التحول الرقمي المتسارع، يكتسي الأمن السيبراني أهمية بالغة لحماية المعطيات وضمان استمرارية الأنشطة الاقتصادية والخدماتية.

وتحرص غرفة التجارة والصناعة والخدمات لجهة طنجة تطوان الحسيمة، عبر هذا الدليل، على تمكين المنتسبين والفاعلين الاقتصاديين من فهم المخاطر الرقمية واتباع ممارسات آمنة.

يشكل هذا الدليل أداة توعوية عملية تعزز من ثقافة الحماية السيبرانية، وترسخ الوعي الجماعي كخط دفاع أول ضد التهديدات الإلكترونية، بما يضمن بيئة رقمية موثوقة ودعماً للاستثمار والتنمية الجهوية.

C.C.I.S
TANGER-TÉTOUAN-AL HOCEIMA

Bonnes Pratiques pour la Sensibilisation à la Cybersécurité

أفضل الممارسات للتوعية بالأمن السيبراني

كلمة السيد الرئيس حول الامن السيبراني

في عالم يتسارع فيه إيقاع التحول الرقمي، لم تعد التحديات الإلكترونية مجرد احتمالات بعيدة، بل أصبحت واقعاً يفرض نفسه على الأفراد والمؤسسات على حد سواء. ومع تنامي الاعتماد على التكنولوجيا في مختلف مناحي الحياة، برز الأمن السيبراني كركيزة أساسية لحماية المعلومات وضمان استمرارية الأعمال والخدمات.

وتماشياً مع التوجيهات الملكية السامية التي تؤكد على ضرورة ترسيخ حكامة فعالة داخل المؤسسات، وتفعيلاً للأدوار الجديدة التي أناطها الدستور بالغرف المهنية، تعمل غرفة التجارة والصناعة والخدمات لجهة طنجة تطوان الحسيمة على تعزيز الوعي بالأمن السيبراني كرافعة لحماية النسيج الاقتصادي الجهوي.

إن المخاطر مثل التصيد الإلكتروني، وهجمات برامج الفدية، واختراق الحسابات نتيجة كلمات مرور ضعيفة، لم تعد حوادث تقنية معزولة، بل تهديدات مباشرة لمصالح المقاولات، ولثقة المواطن والمستثمر. من هنا جاء هذا الدليل الشامل ليواكب حاجيات المنتسبين والفاعلين الاقتصاديين ، ويوفر محتوى عملياً مبسطاً حول التهديدات الشائعة، وأساليب الحماية، وما يجب القيام به عند حدوث اختراق أو محاولة هجوم.

كما يشكل هذا الدليل امتداداً للدور التأطيري الذي تضطلع به الغرفة، ويعكس انخراطها الفعلي في ترسيخ ثقافة رقمية مسؤولة داخل المقاولات والإدارات، عبر تبني ممارسات حديثة تواكب متطلبات العصر الرقمي.

واثقون أن تعميم التوعية السيبرانية وتبني ممارسات رقمية آمنة سيشكلان حجر الزاوية لبناء بيئة اقتصادية جهوية آمنة، تنافسية، ومتوافقة مع المعايير الرقمية الدولية.

فلنعمل جميعاً على ترسيخ هذا الوعي داخل مقاولاتنا ومؤسساتنا، وجعل الأمن السيبراني أولوية يومية، تضمن الحماية وتفتح آفاقاً جديدة للتنمية والاستثمار.

السيد عبد اللطيف أفيلال

رئيس غرفة التجارة و الصناعة و الخدمات لجهة
طنجة - تطوان - الحسيمة

C.C.I.S
TANGER-TÉTOUAN-AL HOCEIMA

Bonnes Pratiques pour la Sensibilisation à la Cybersécurité

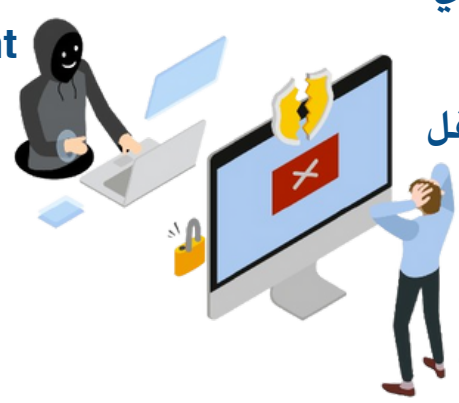
أفضل الممارسات للتوعية بالأمن السيبراني

Pourquoi la cybersécurité est-elle importante ?

Dans un monde de plus en plus connecté, protéger les données personnelles et professionnelles est essentiel. Une seule erreur peut exposer toute l'organisation à des cyberattaques coûteuses.

Principales menaces à connaître :

- **Phishing : emails ou SMS piégés**
- **Ransomware : logiciels qui bloquent vos fichiers**
- **Ingénierie sociale : manipulation humaine**
- **Fuite de données : vol ou perte de fichiers sensibles**
- **Piratage de comptes : à cause de mots de passe faibles**



أبرز التهديدات الإلكترونية :

- التصيد (Phishing) عبر البريد الإلكتروني أو الرسائل النصية
- برامج الفدية (Ransomware) التي تقفل ملفاتك وتطلب المال
- الهندسة الاجتماعية التحكم البشري
- تسريب البيانات بسبب السرقة أو الإهمال
- اختراق الحسابات نتيجة لكلمات مرور ضعيفة

En cas d'incident :

- **Gardez votre calme 😌**
- **Déconnectez l'appareil d'Internet**
- **Contactez immédiatement un spécialiste en Cybersécurité**
- **Ne tentez pas de résoudre seul sans signaler**

ماذا تفعل في حالة حدوث هجوم ؟

- لا تصب بالذعر
- افصل الجهاز عن الإنترنت فوراً
- تواصل مباشرة مع خبير في الأمن السيبراني
- لا تحاول الإصلاح بنفسك دون الإبلاغ

Bonnes pratiques à adopter :

- 🔑 **Utilisez des mots de passe forts et uniques**
- 🔄 **Activez la vérification en deux étapes (2FA)**
- 📥 **Ne téléchargez pas de fichiers inconnus**
- 🚫 **Ne cliquez jamais sur des liens suspects**
- 🔄 **Faites des sauvegardes régulières**

نصائح للحماية :

- استعمل كلمات مرور قوية ومختلفة
- فعّل المصادقة الثنائية (2FA)
- لا تقم بتنزيل ملفات مشبوهة
- لا تضغط على الروابط المشكوك فيها
- قم بحفظ نسخ احتياطية دورية

C.C.I.S
TANGER-TÉTOUAN-AL HOCEIMA

Sensibilisation à la Cybersécurité (Ingénierie Sociale)

التوعية بالأمن السيبراني (الهندسة الاجتماعية)

Qu'est-ce que l'ingénierie sociale ?

L'ingénierie sociale est une technique utilisée par les cybercriminels pour manipuler les personnes afin qu'elles divulguent des informations sensibles, ouvrent une porte d'accès, ou contournent des procédures de sécurité, souvent sans s'en rendre compte.

Objectifs des attaquants :

- Voler des mots de passe, fichiers, ou identifiants
- Obtenir un accès physique ou à distance à votre système
- Installer des malwares à travers des manipulations humaines

أهداف المهاجم :

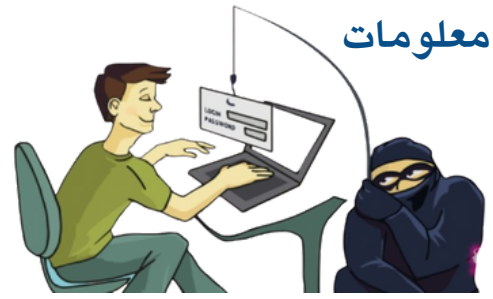
- سرقة كلمات المرور أو الملفات أو الوصول إلى الشبكة
- الدخول المادي إلى المكتب أو النظام
- تثبيت برامج ضارة عبر تفاعل بشري

Formes courantes d'attaques :

- Phishing : emails qui imitent des services légitimes
- Appels frauduleux se faisant passer pour l'IT, la banque, etc.
- Visites physiques (quelqu'un entre dans les bureaux en prétendant être un technicien)
- Collecte d'infos sur les réseaux sociaux pour personnaliser l'attaque

أنواع الهجمات الشائعة :

- التصيد الإلكتروني (Phishing) عبر البريد الإلكتروني
- مكالمات مزيفة من شخص يدّعي أنه من الدعم التقني أو البنك
- زيارات شخصية مشبوهة (شخص يتظاهر بأنه تقني أو موظف)
- استعمال مواقع التواصل الاجتماعي لجمع معلومات مسبقة



Comment se protéger ?

- Ne partagez jamais d'informations sensibles (par téléphone, mail ou en personne)
- Vérifiez toujours l'identité de l'appelant ou du visiteur
- Soyez discret sur les réseaux sociaux professionnels

كيف نحمي أنفسنا ؟

- لا تشارك معلوماتك الحساسة مع أي شخص
- تحقق دائماً من هوية المتصل أو الزائر
- لا تكشف الكثير عن نفسك على الإنترنت

C.C.I.S
TANGER-TÉTOUAN-AL HOCEIMA

Sensibilisation à la Cybersécurité (Prévention contre le Phishing)

التوعية بالأمن السيبراني (الحماية من التصيد الإلكتروني)

Qu'est-ce que l'attaque de Phishing ?

Le phishing est une tentative de fraude où des attaquants vous incitent à cliquer sur des liens malveillants, à télécharger des fichiers dangereux, ou à divulguer vos identifiants, mots de passe ou informations personnelles.

Signes courants d'un email frauduleux

- Urgence exagérée : "Votre compte sera supprimé !"
- Fautes d'orthographe ou de grammaire
- Adresse email douteuse de l'expéditeur
- Liens suspects (vérifiez en survolant avant de cliquer)
- Pièces jointes inattendues
- Faux messages d'un établissement ou banques

Que faire si vous recevez un email suspect ?

- Ne cliquez sur aucun lien
- Ne répondez pas au message
- Signalez-le immédiatement au spécialiste en Cybersécurité
- Supprimez l'email après vérification

Conseils pour se protéger :

- Utilisez des mots de passe complexes et uniques
- Activez l'authentification à deux facteurs (2FA)
- Mettez régulièrement à jour vos logiciels
- Ne partagez jamais vos informations sensibles
- Soyez toujours vigilant en ligne

علامات البريد الإلكتروني الاحتيالي:

- رسائل طارئة ومخيفة: "سيتم إغلاق حسابك!"
- أخطاء إملائية أو نحوية
- عنوان بريد إلكتروني مشبوه للمرسل
- روابط غير واضحة (تحقق منها قبل النقر)
- مرفقات غير متوقعة
- رسائل مزيفة من البريد الالكتروني للادارة

ماذا تفعل عند الشك في رسالة تصيد؟

- لا تنقر على أي رابط
- لا ترد على الرسالة
- قم بالإبلاغ فوراً لخبير في الأمن السيبراني
- احذف الرسالة بعد التأكد منها

نصائح للحماية :

- استعمل كلمات مرور قوية ومختلفة
- فعّل المصادقة الثنائية (2FA)
- حدّث برامجك بانتظام
- لا تشارك معلوماتك الحساسة
- كن دائماً يقظاً على الإنترنت

C.C.I.S
TANGER-TÉTOUAN-AL HOCEIMA

Sensibilisation à la Cybersécurité (Protection contre les Ransomwares)

التوعية بالأمن السيبراني (الحماية من برامج الفدية)

Qu’est-ce qu’un Ransomware ?

Un ransomware est un logiciel malveillant qui bloque l’accès à vos fichiers ou systèmes et demande une rançon pour les déverrouiller.

Comment les ransomwares vous infectent-ils ?

- Pièces jointes dans des emails suspects
- Sites web piégés ou téléchargements infectés
- Clés USB inconnues
- Mots de passe faibles ou ordinateurs non protégés

كيف تصيبك برامج الفدية ؟

- مرفقات في رسائل بريد إلكتروني مشبوهة
- زيارة مواقع ضارة أو تحميل ملفات غير آمنة
- مفاتيح USB من مصادر غير موثوقة
- كلمات مرور ضعيفة أو برامج غير محدثة

Risques :

- Perte totale de fichiers (documents, photos, projets…)
- Interruption du travail ou des services
- Perte de données confidentielles
- Dommages financiers ou réputationnels

المخاطر :

- فقدان كامل للملفات والبيانات
- توقف العمل أو الخدمات
- تسرب معلومات حساسة
- خسائر مالية وتشويه السمعة

Que faire pour se protéger ?

- Ne jamais ouvrir des pièces jointes suspectes
- Effectuer des sauvegardes régulières
- Garder les logiciels à jour
- Utiliser un antivirus à jour
- Ne jamais payer la rançon – cela ne garantit rien !
- En cas d’incident, signalez immédiatement au spécialiste en Cybersécurité

كيف تحمي نفسك ؟

- لا تفتح أي مرفق مشبوه
- قم بعمل نسخ احتياطية بانتظام
- حدّث برامجك وأنظمتك باستمرار
- استعمل برنامج مضاد للفيروسات
- لا تدفع الفدية أبداً!
- في حالة حدوث هجوم، تواصل فوراً مع خبير في الأمن السيبراني