الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة 20 أوت 1955 – سكيكدة

برنامج الأيام التحسيسية حول المخاطر السبيرانية

المتعلقة باستعمال وسائل التواصل الاجتماعي

من 05 إلى 10 ماي 2024

يـوم الأحد 05 ماي- 2024: - مـركـز أنظمـة شبكـات الإعلام والاتصال –

افتتاح نشـاطـات الأيـام التحسيسيـــة

- ✓ مداخلة السيد مدير الجامعة البروفيسور بوفندي توفيق كلمه حول أهمية هذه الأيام التحسيسية.
- ✓ مداخلة البروفيسور معزوزي إسماعين حول الهجمات السبيرانية: المخاطر و وسائل الحماية.
- ✓ نقاش مفتوح بحضور عمداء الكليات وخلايا الأمن المعلوماتي للجامعة.

يوم الثلاثاء 07 -05- 2024 - قاعة المحاضرات للمكتبة المركزية للجامعة – الساعة 10 إلى 12

يوم إعلامي حول المخاطر السبيرانية يتـضمـــن:

- ✓ كلمة افتتاحية للسيد : مدير الجامعة البروفيسور بوفندي توفيق .
- ✓ مداخلة البروفيسور : معزوزي إسماعين بعنوان الهجمات السبيرانية: المخاطر ووسائل الحماية.
- ✓ مداخلة السيد: مراقب الشرطة رئيس أمن ولاية سكيكدة: العواقب الناتجة عن مخاطر الأمن السبيراني .

- ✓ مداخلة السيد : قائد فرقة الدرك الوطني : العواقب السلبية الناتجة عن المخاطر السبيرانية.
- ✓ مداخلة الدكتور : لعور عاشور: "الإدمان الرقمي وتأثيره على التشوه المعرفي والقيمي.

يوم الثلاثاء 07 - 05 -2024: مركز أنظمة الشبكات - الساعة 13سا إلى 16سا

ورشة عمل تجمع رئيس مركز أنظمة الشبكات مع مسؤولي صفحات التواصل الاجتماعي للجامعة.

يومي الأربعاء و الخميس 08 و09 ماي -2024:

نشاطات مكاتب خلايا الأمن المعلوماتي للجامعة.

- ✓ وضع خلايا الأمن المعلوماتي للكليات للتواصل المباشر مع موظفي الجامعة حيث تقوم بمعاينة استبيان المستخدمين لأهم المخاطر وتوزيع استمارة استجواب حول أهم المخاطر وتوزيع مطويات تحسيسية للمخاطر السبيرانية.

وزارة التعليم العالي والبحث العلمي

جامعة 20 أوت 1955 - سكيكدة

مركز الأنظمة والشبكات خلية الأمن المعلوماتي

استخدام شبكات التواصل الاجتماعي وإدارة الصفحات الرسمية للمؤسسة الجامعية بشكل إيجابي وآمن

الأمن المعلوماتي مسؤولية الجميع

2024

مقدمة :

في ظل انتشار استخدام مواقع التواصل الاجتماعي بين الطلبة وأعضاء الأسرة الجامعية، بات من الضروري نشر الوعي حول فوائدها وكذلك مخاطرها، وكيفية الاستخدام الآمن والمسؤول لهذه المنصات.

تهدف هذه المطوية إلى توعية مكونات الأسرة الجامعية وخاصة مسؤولي الصفحات الرسمية للجامعة بأهمية استخدام مواقع التواصل الاجتماعي بشكل إيجابي، وتعريفهم بالمخاطر التي قد يتعرضون لها، وكيفية حماية أنفسهم وبيانات المؤسسة من مخاطر الأمن المعلوماتي والهندسة الاجتماعية.

أهمية استخدام مواقع التواصل الاجتماعي للمؤسسة الجامعية :

- **التواصل مع أعضاء الأسرة الجامعية وخاصة الطلبة :**
  - مشاركة أخبار الجامعة وإنجازاتها.
  - الرد على استفسارات الطلبة ومعالجة انشغالاتهم.
  - الحصول على ملاحظات الطلبة حول البرامج والخدمات.
- **بناء مجتمع جامعي :**
  - خلق شعور بالانتماء بين الطلبة وأعضاء الهيئة التدريسية والإدارية.
  - تشجيع التفاعل والمشاركة بين أعضاء الأسرة الجامعية.
- **الترويج للجامعة :**
  - زيادة التعريف بالجامعة وبرامجها وأنشطتها.
  - جذب الطلبة الجدد وحتى الأجانب.
  - تعزيز علاقات الجامعة مع المجتمع.
- **التعاون البحثي :**
  - التواصل مع الباحثين من جامعات أخرى.
  - مشاركة الأبحاث والنتائج العلمية.
  - جذب التمويل للأبحاث والمشاريع.

مخاطر استخدام مواقع التواصل الاجتماعي للمؤسسة الجامعية :

- **مخاطر الأمن المعلوماتي :**
  - سرقة البيانات الشخصية للطلبة وأعضاء الأسرة الجامعية.
  - اختراق الحسابات الرسمية للجامعة.
  - نشر المعلومات المضللة والكاذبة عن الجامعة.

- **مخاطر الهندسة الاجتماعية :**
  - خداع مسؤولي الصفحات الرسمية لكشف معلومات حساسة عن الجامعة.
  - نشر محتوى ضار باسم الجامعة.
  - الإضرار بسمعة الجامعة.
- **مخاطر الخصوصية :**
  - جمع البيانات الشخصية للطلاب دون علمهم أو موافقتهم.
  - استخدام البيانات الشخصية لأغراض غير قانونية.
  - الإضرار بخصوصية الطلبة.

احتياطات الأمن المعلوماتي وخاصة مسؤولي الصفحات الرسمية :

- **حماية الحسابات :**
  - استخدام كلمة مرور قوية وفريدة لكل حساب وتحيينها دوريا.
  - تفعيل المصادقة الثنائية للولوج.
  - عدم مشاركة معلومات تسجيل الدخول مع أي شخص.
  - الحذر من الروابط والملفات المشبوهة.
  - استخدام برامج مكافحة الفيروسات ومكافحة البرامج الضارة.
- **حماية البيانات :**
  - عدم نشر معلومات شخصية للطلبة أو أعضاء الأسرة الجامعية على صفحات الجامعة.
  - الحذر من المعلومات التي يتم مشاركتها مع الجمهور.
  - حذف أي بيانات شخصية غير ضرورية.
- **حماية المحتوى :**
  - عدم نشر أي محتوى دون موافقة الإدارة.
  - عدم نشر محتوى محمي بحقوق النشر دون إذن.
  - الإبلاغ عن أي محتوى مسيء أو ضار إلى إدارة صفحة التواصل الاجتماعي.
- **الوعي بأساليب الهندسة الاجتماعية الشائعة :**
  - مثل التظاهر بكونهم طلابًا أو أعضاء هيئة تدريسية أو موظفين حكوميين، أو إرسال رسائل بريد إلكتروني مزيفة تبدو وكأنها من مصدر موثوق.

- لا تتواصل مع أشخاص لا تعرفهم أو لا تثق بهم.
- لا تشارك معلومات حساسة مع أي شخص، حتى لو بدا أنه شخص تعرفه أو تثق به.

- **إنشاء سياسة استخدام واضحة لمواقع التواصل الاجتماعي :**
  - تحدد هذه السياسة قواعد استخدام مواقع التواصل الاجتماعي من قبل مسؤولي الصفحات الرسمية والطلبة وأعضاء الهيئة التدريسية.
  - يجب أن تتضمن السياسة قواعد حول المحتوى المسموح به والمحتوى المحظور، وكيفية التعامل مع المخالفات.
- **تدريب موظفي المؤسسة حول كيفية استخدام مواقع التواصل الاجتماعي بشكل آمن :**
  - يجب أن يتضمن التدريب معلومات حول مخاطر الأمن المعلوماتي والهندسة الاجتماعية، وكيفية استخدام مواقع التواصل الاجتماعي بشكل مسؤول.
- **إنشاء نظام للإبلاغ عن أي مخالفات :**
  - يجب أن يسهل على الطلبة وأعضاء الهيئة التدريسية الإبلاغ عن أي محتوى مسيء أو ضار أو سلوك غير لائق على صفحات الجامعة الرسمية.
- **مراقبة صفحات الجامعة الرسمية بانتظام :**
  - يجب على مسؤولي الصفحات الرسمية مراقبة صفحات الجامعة بحثًا عن أي نشاط مشبوه.
- **الاستجابة بسرعة لأي مخالفات :**
  - يجب على مسؤولي الصفحات الرسمية اتخاذ إجراءات سريعة للتعامل مع أي مخالفات، مثل إزالة المحتوى المسيء أو حظر المستخدمين الذين يتصرفون بشكل غير لائق.
- **البقاء على اطلاع على أحدث التهديدات الأمنية :**
  - يجب على مسؤولي الصفحات الرسمية البقاء على اطلاع على أحدث التهديدات الأمنية على مواقع التواصل الاجتماعي، واتخاذ خطوات لحماية صفحات الجامعة من هذه التهديدات.

يبقى أعضاء خلية الأمن المعلوماتي للجامعة على مستوى الكليات ومركز الأنظمة والشبكات في خدمتكم. فلا تترددوا في الاتصال في أي حالة شك.

Université 20 août 1955 – Skikda

Centre des systèmes et réseaux d'information et de communication, de télé-enseignement et d'enseignement à distance

Sécurité informatique

Sensibilisation et bonnes pratiques

Cellule de sécurité informatique - 2024

Introduction

Depuis plusieurs années, les entreprises redoutent les attaques informatiques, et considèrent les comme une vraie menace.

Aujourd'hui, la sécurité est devenue un aspect primordial du système d'information **(SI)** d'une entreprise, voire même incontournable dans un monde où la donnée est devenue de « l'Or».

Définition

La **sécurité des systèmes d'information** (**SSI**) ou plus simplement **sécurité informatique**, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du SI.

Les risques et l'importance de la sécurité

Le système d'information constitue un patrimoine essentiel des entreprises. Constitué d'un ensemble de ressources matérielles et logicielles, il permet de traiter, stocker et transférer les données des entreprises. Ainsi la sécurité des systèmes d'information cherche à apporter une meilleure maîtrise des risques qui pèsent réellement sur l'entreprise et répondre à certains enjeux qu'on peut résumer en 4 lettres « DICA » (Disponibilité, Intégrité, Confidentialité et Auditabilité).

- **Disponibilité :** garantir l'accès aux ressources, au moment voulu, aux personnes habilitées d'accéder à ces ressources.
- **Intégrité :** garantir que les données échangées sont exactes et complètes.
- **Confidentialité :** garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources de l'entreprise.
- **Auditabilité :** garantir la traçabilité des accès et des tentatives d'accès et la conservation de ces traces comme preuves exploitables.

En général, la sécurité informatique consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées pour les fins auxquelles elles ont été conçues au début.

Règles d'utilisation des SI et bonnes pratiques

Face à la récurrence des piratages non ciblés, les entreprises commencent à mettre en place des **systèmes de sécurisation** pour faire face à ces menaces de plus en plus fréquentes. Alors, quelles sont les bonnes pratiques à adopter ?

Nous avons voulu faire un focus sur les bons réflexes à acquérir afin de maintenir votre **système informatique** en bonne santé.

- **Messagerie électronique**
  - ✓ Il peut ici être rappelé que la messagerie doit être utilisée à des fins professionnelles et que tout message envoyé ou reçu depuis le poste de travail fourni par l'employeur est considéré comme étant de nature professionnelle.
  - ✓ En outre, au vu du principe de proportionnalité, n'utilisez pas la messagerie professionnelle pour : créer des comptes sociaux (Facebook, Twitter, etc).
  - ✓ Il est strictement interdit d'ouvrir les spam et en général les messages de sources inconnus.
  - ✓ Ne jamais relayer des canulars ou cliquer sur un lien dans un email demandant l'authentification.
  - ✓ Ne pas ouvrir les courriers électroniques douteux ou d'expéditeurs inconnus.
- **L'accès à Internet**
  - ✓ On rappelle que la connexion Internet mise à disposition par l'employeur doit être utilisée à des fins professionnelles mais qu'un usage privé est toléré dans la mesure où il reste raisonnable. Le critère permettant de déterminer ce caractère raisonnable peut être une durée de connexion au-delà de laquelle l'utilisation d'Internet à titre privé sera considérée comme excessive.
  - ✓ Il est interdit d'utiliser les clés de connexion à internet tel que « Mobiconnect » ou bien un modem par l'employé sur le poste de travail fournis par l'entreprise.
  - ✓ L'utilisation d'Internet est limitée pour des raisons de sécurité.

L'accès est restreint (filtre web), mais suffisant pour votre usage professionnel.

- ✓ Téléchargez uniquement des fichiers nécessaires à votre travail, jamais pour votre loisir, et soyez attentifs aux fichiers reçus.

• Utilisation des réseaux sociaux

- ✓ Ne jamais utiliser la messagerie professionnelle pour créer des comptes sociaux (Facebook, Twitter, etc).
- ✓ Ne diffusez pas vos informations professionnelles (établissement, grade…) sur vos profils.
- ✓ Si vous avez besoin d'aide, ne communiquer pas des informations professionnelles vous concernant (établissement, poste occupé, systèmes utilisés…).

• Les logiciels et les applications

Si vous téléchargez du contenu numérique sur des sites internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie.

Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données, lancer des attaques, …etc.

Dans ce contexte, et afin de veiller à la sécurité de votre machine et de vos données :

- ✓ Téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
- ✓ Ne jamais ouvrir les pièces jointes avec les extensions : .pif, .com ; .bat ; .exe ; .vbs ; .lnk …
- ✓ Pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- ✓ Restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens ;
- ✓ Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir.

• Gestion des mots de passe

La notion de sécurité nécessite également quelques actions de la part de l'entreprise et des utilisateurs. La première est le **renouvellement régulier des mots de passe**, et d'utiliser différents mots de passe selon les comptes, et la **complexification** de celui-ci afin d'éviter la compromission.

- ✓ Pour créer un mot de passe correct, relativement difficile à « brute-forcer », il est recommandé qu'il soit composé d'au moins 8 caractères avec des minuscules, majuscules, chiffres et caractères spéciaux.
- ✓ N'écrivez jamais vos mots de passe sur un bout de papier, à moins de le conserver sous clé.
- ✓ N'utilisez pas de mots de passe contenant le nom, le numéro de passeport, ou la date de naissance, …etc.
- ✓ Ne communiquez jamais votre mot de passe à quiconque, même pas à votre patron.

• La sécurité physique

- ✓ Afin de se protéger des dégâts des eaux, tout équipement sensible ne doit pas être placé en rez-de-chaussée ou sous-sol.
- ✓ Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux dans lesquels résident les informations de l'unité.
- ✓ Les locaux contenant des informations sensibles et des moyens de traitement de l'information (salles serveurs, secrétariat de direction ou comptable, service pédagogique …) doivent donc être protégés physiquement des accès incontrôlés ou malveillants (verrouillé avec des clés, ordinateur verrouillé par mots de passe).
- ✓ Mettre en œuvre le port du badge permettant de différencier les employés des visiteurs extérieurs (stagiaires, intérimaires, prestataires, visiteurs…).

• La mobilité

- ✓ Se méfier des clés USB, disques durs externes… notamment s'il n'en est pas le propriétaire.
- ✓ De retour d'un déplacement professionnel, avant de connecter l'ordinateur portable au réseau de l'entreprise, le confier à une personne qualifiée qui s'assurera de son intégrité.
- ✓ A l'extérieur de l'entreprise, surveiller de manière constante son ordinateur portable. Ne jamais le laisser dans le coffre de sa voiture, dans une chambre d'hôtel, ou dans la salle de travail durant les pauses.
- ✓ Utiliser de préférence du matériel dédié aux missions (ordinateurs, téléphones, supports amovibles, etc.). Ces appareils ne doivent contenir aucune information autre que celles utiles pour la mission.

• Les mises à jour et les sauvegardes

- ✓ Le premier réflexe, et le plus évident, est de mettre à jour le système d'exploitation, les logiciels et la solution antivirus de tous les postes. Cette « réactualisation » permet la correction de failles critiques, l'amélioration de la protection et une diminution de la surface d'attaque. Les mises à jour participent donc à une augmentation de la fiabilité du système d'information.
- ✓ L'attaque dite « Ransomware » consiste en l'intrusion d'un logiciel malveillant, qui chiffrera l'ensemble des données d'un ordinateur (et potentiellement des lecteurs réseaux connectés), obligeant l'utilisateur à payer une rançon pour récupérer ses données.
- ✓ Cette attaque est d'autant plus vicieuse pour une entreprise du fait de la nature des données stockées. La meilleure façon de se prémunir de cette attaque est d'effectuer des sauvegardes régulières afin d'avoir toujours une copie des données « propre » à disposition.
- ✓ Il existe différentes manières de perdre des données : elles peuvent être écrasées par erreur, rendues illisibles à cause d'un défaut sur le disque dur, voire détruites par un incendie ou un dégât des eaux. Vous pouvez éviter de tels désagréments en faisant régulièrement des backups de vos données.

• L'utilisation d'antivirus

- ✓ Installez un programme antivirus sur les postes de travail (clients) et ordinateurs portables, et effectuez régulièrement les mises à jour (une fois par jour minimum).
- ✓ Interdisez expressément la désactivation, même temporaire, du programme antivirus.
- ✓ Demandez à vos collaborateurs de signaler immédiatement au responsable informatique les messages d'avertissement virus.
- ✓ Effectuez au moins une fois par semaine un scan complet de votre disque dur.