LES RISQUES DE CYBER ATTAQUE

Avant : j'assure la sécurité de mes systèmes informatiques

Je peux m'initier à la cyber-sécurité et approfondir mes connaissances en participant au MOOC (cours en ligne) https://secnumacademie.gouv.fr/

Je choisis avec soin mes mots de passe : entrer un mot de passe permettant de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable est un geste quotidien de sécurité.

Choisir un mot de passe difficile à déceler par une tierce personne ou par du piratage informatique est ainsi un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

Comment bien choisir son mot de passe ?

- **Définissez des mots de passe composés d'au moins 12 caractères** :
  - Mélangeant majuscules, minuscules, chiffres et caractères spéciaux,
  - N'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance,
  - Ne formant pas de mots figurant dans le dictionnaire.
- **N'utilisez pas le même mot de passe pour tout**, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle,
- Méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe.

Entretenir régulièrement vos appareils numériques

Mettre à jour régulièrement les logiciels de vos appareils numériques.

Dans chaque système d'exploitation (Android, MacOS, Linux, Windows…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité.

Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations longtemps encore après leur découverte ou même leur correction. Il donc nécessaire de procéder aux mises à jour régulières des logiciels.

Comment faire ?

- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible,
- Ou téléchargez les correctifs de sécurité disponibles en utilisant pour cela exclusivement les sites Internet officiels des éditeurs.

J'effectue couramment des sauvegardes

Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur.

Comment faire ?

Utilisez des supports externes tels qu'un disque dur externe, un CD ou un DVD enregistrable pour enregistrer et sauvegarder vos données.

Je prends soin de mes informations personnelles et de mon identité numérique

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.

Une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet, exemple **jamais votre Banque ne vous demandera de lui préciser votre numéro de compte ou de carte bancaire avec son code** :

- Soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données, par exemple avec des partenaires commerciaux,
- Ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux,
- Utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…).

Je sécurise mon WIFI

Si l'utilisation du Wi-Fi est une pratique attractive, elle permet, lorsque le point d'accès n'est pas sécurisé, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes.

C'est pour cette raison que l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise.

Le Wi-Fi, solution pratique et peu coûteuse, peut cependant être le seul moyen possible d'accéder à Internet. Il convient dans ce cas de sécuriser l'accès en configurant votre box :

- Modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet,

- Vérifiez que votre box dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes),
- Modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents,
- Ne divulguez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement,
- Activez et configurez les fonctions pare-feu / routeur,
- Désactivez le Wi-Fi de votre borne d'accès lorsqu'il n'est pas utilisé.

Je sépare mes usages personnels et professionnels

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone…) personnels et professionnels.

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- Ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles,
- Ne stockez pas de données professionnelles sur vos équipements communicants personnels,
- Evitez de connecter des supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

Je suis aussi prudent avec mon smartphone ou ma tablette qu'avec mon ordinateur

Bien que proposant des services innovants, les smartphones ou tablettes sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires d'hygiène informatique :

- N'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer,
- En plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement,
- Effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre smartphone ou de votre tablette.

Je suis prudent lorsque j'ouvre mes messages électroniques

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, phishing/hameçonnage, pièces jointes piégées…).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- L'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message,
- **N'ouvrez pas les pièces jointes provenant de destinataires inconnus** ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts,
- Si un lien ou plusieurs figurent dans un courriel, **vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer**. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer,
- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : données bancaires)
- N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

Je suis vigilant lors d'un paiement sur Internet

Lorsque vous réalisez des achats en ligne, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur.

Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs),
- Assurez-vous que la mention « **https://** » apparait au début de l'adresse du site Internet,
- Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple,
- Si possible, lors d'un achat en ligne, privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS,
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire.

Je télécharge les programmes et logiciels sur les sites officiels des éditeurs

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 personnelles, lancer des attaques, etc…

C'est la raison pour laquelle il est vivement recommandé de :

- Télécharger vos programmes sur les sites officiels des éditeurs,

- Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir, afin de vérifier qu'ils ne sont pas infectés par un quelconque virus ou spyware.

Si je suis victime d'une cyber-attaque : je fais un signalement auprès des autorités

Suite à une escroquerie ou une cyber-attaque, déposez plainte auprès d'un service de Police nationale ou de Gendarmerie nationale ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Contactez votre Banque le plus rapidement possible.

Munissez-vous de tous les renseignements suivants :

- Références du (ou des) transfert(s) d'argent effectué(s),
- Références de la (ou des) personne(s) contactée(s) : adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés...
- Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux,
- Tout autre renseignement pouvant aider à l'identification de l'escroc.

Vous pouvez signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » (https://www.internet-signalement.gouv.fr) ou le numéro dédié :

0811 02 02 17

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme https://www.cybermalveillance.gouv.fr/.

Cette plateforme dispose d'outils et propose des démarches de sensibilisation.

Des services spécialisés se chargent ensuite de l'enquête :

- Police nationale : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC),
- Gendarmerie nationale : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC).