12 RÈGLES FONDAMENTALES DE SÉCURITÉ INFORMATIQUE

CAHIER DU CIRB 36

GUIDE PRATIQUE


CRIME SCENE-DO NOT ENT

En tant qu'administration publique, vous êtes conscients que les cybercriminels peuvent aussi frapper chez vous. Que l'objectif de ces criminels soit de détruire des données ou d'extorquer de l'argent, les conséquences potentielles d'infractions graves à votre sécurité informatique sont à prendre très au sérieux.

Le secteur public doit se montrer irréprochable quand il s'agit de protection informatique. Nous sommes en effet encore davantage sous les feux de la presse et de l'opinion publique en cas de problème. Et c'est normal. Nous traitons en effet souvent les données privées de nombreux citoyens.

Autrement dit, une organisation publique telle que la vôtre doit protéger suffisamment ses systèmes informatiques au moyen d'un plan de sécurité professionnel. Nous voulons vous y aider.

Le Centre d'Informatique pour la Région bruxelloise, depuis plus de 25 ans déjà, est le support de votre politique informatique. Nous aimerions aujourd'hui franchir un pas de plus et vous soutenir aussi dans la mise sur pied d'un plan de sécurité informatique professionnel.

Au travers de ce petit guide pratique, nous vous recommandons d'ores et déjà un certain nombre de bonnes pratiques très peu coûteuses, faciles à mettre en œuvre et qui éliminent une bonne partie des risques.

Hervé FEUILLIEN
Directeur général

Robert HERZEELE
Directeur général adjoint


CONNECT
click
credit
PAY
ON
PAY CREDIT CARD
CLOUD
Protection!
DATA
DATA
Lock!
LOG IN :
USERNAME
PASSWORD

SOMMAIRE

POURQUOI UN PLAN DE SÉCURITÉ INFORMATIQUE ?

PC, portables, tablettes, smartphones font aujourd'hui partie de notre quotidien, tant privé que professionnel. Souvent, on perd de vue les règles élémentaires qui s'imposent dans l'utilisation de ces appareils. Les nouvelles technologies entraînent en effet aussi de nouveaux risques.

Les données sensibles (données privées des citoyens, contrats, projets en cours...) peuvent être dérobées par des pirates informatiques ou récupérées en cas de perte ou vol d'un PC, d'un smartphone, d'une tablette ou d'un ordinateur portable. Ces scénarios entraînent des pertes économiques et financières et dégradent l'image de l'ensemble de votre organisation.

Ces dangers peuvent néanmoins être assez bien maîtrisés grâce à un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre immédiatement dans votre organisation.

Partagez-les avec vos collaborateurs, placez-le sur votre intranet, afin qu'eux aussi prennent conscience de l'importance de la sécurité informatique.

1. CHOISIR AVEC SOIN SES MOTS DE PASSE

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour protéger suffisamment vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne.

QUELQUES RÉGLES FONDAMENTALES

- N'utilisez pas de mots de passe courts. Huit caractères sont un minimum. Plus, c'est encore mieux.
- Préférez des mots de passe combinant des majuscules, minuscules, chiffres et caractères spéciaux.
- Évitez des références personnelles dans vos mots de passe (nom, date de naissance, nom de votre animal, etc.). Ils sont souvent plus faciles à trouver que vous ne le pensez.
- Utilisez de préférence de mots qui ne figurent pas dans le dictionnaire, donc difficiles à trouver par des robots de recherche.
- Veillez à changer régulièrement vos mots de passe.
- Ne conservez jamais vos mots de passe dans un fichier non protégé ou sur un bout de papier.
- Ne permettez pas au navigateur de mémoriser vos mots de passe si vous utilisez un ordinateur public ou partagé, par exemple dans un cybercafé.
- Consignez les règles au sein de votre organisation dans des directives et communiquez-les clairement. Veillez aussi à ce que ces directives soient respectées.

2. METTRE À JOUR RÉGULIÈREMENT VOS LOGICIELS

Dans chaque système d'exploitation (Android, iOS, MacOS, Linux, Windows,...), logiciel ou application, il y a des faiblesses que les cybercriminels peuvent exploiter. Habituellement, les éditeurs de logiciels publient régulièrement des mises à jour de sécurité pour corriger ces faiblesses. Pourtant, il y a encore et toujours trop d'utilisateurs qui n'installent pas ces mises à jour.

QUELQUES RÉGLES FONDAMENTALES

- Veillez à ce que toutes les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, vous devrez télécharger et installer vous-même manuellement les correctifs de sécurité disponibles, ce qu'on oublie souvent de faire.
- Utilisez exclusivement les sites Internet officiels des éditeurs.
- Utilisez exclusivement des systèmes d'exploitation récents pour lesquels des mises à jour sont encore diffusées.
- Définissez et faites appliquer réellement et strictement une politique de mise à jour au sein de votre organisation.

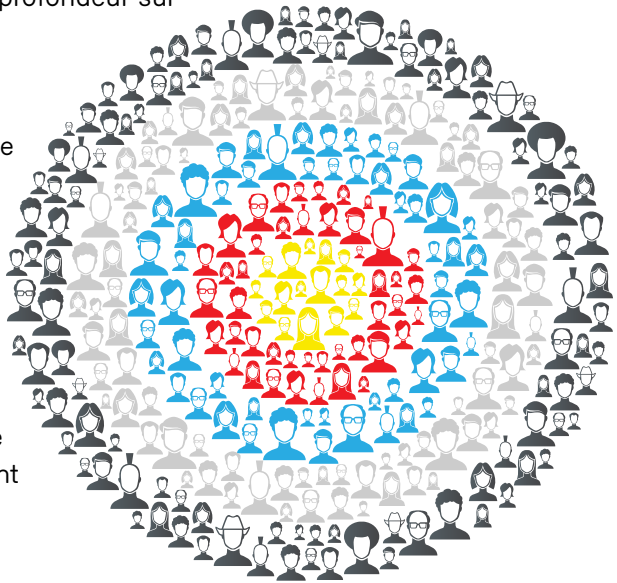
3. QUI SONT MES UTILISATEURS ?

Lorsque vous accédez à votre ordinateur, vous bénéficiez de certains droits d'utilisation sur celui-ci. On distingue généralement les droits « d'utilisateur » et les droits dits « d'administrateur ».

- Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels bureautiques...), un compte utilisateur suffit.
- Le compte administrateur sert à modifier le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels...). Le compte administrateur permet d'effectuer des interventions en profondeur sur votre ordinateur.

QUELQUES RÉGLES FONDAMENTALES

- Veillez à ce que tous les collaborateurs ne consultent que leur propre compte utilisateur ordinaire.
- Veillez à ce que seuls les collaborateurs du service informatique disposent de droits d'administrateur.
- Prévoyez une **procédure d'entrée** pour attribuer correctement et précisément aux nouveaux collaborateurs les droits d'accès aux systèmes informatiques.
- Une **procédure de sortie** est également importante afin de retirer leurs droits d'accès aux collaborateurs qui quittent votre organisation.



4. EFFECTUER DES SAUVEGARDES RÉGULIÈRES

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires). Vous pourrez ainsi récupérer vos données en cas de défaillance ou si vous êtes victime d'un cyberattaque.

Pour les sauvegardes de vos données, vous pouvez utiliser des supports externes, comme un disque dur amovible, une clé USB ou encore un CD ou DVD réinscriptible. Ne les conservez jamais à proximité de votre ordinateur et rangez-les en lieu sûr. Vous éviterez de cette façon que la sauvegarde puisse être détruite par le feu ou emmenée en même temps que l'ordinateur en cas de vol.

QUELS CONSEILS SUPPLÉMENTAIRES

- N'utilisez pas de services « cloud » pour sauvegarder des données confidentielles, sauf si la confidentialité en est garantie, par exemple auprès du Centre d'Informatique pour la Région bruxelloise.
- Veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement.

5. SÉCURISER VOTRE RÉSEAU WIFI

Le wifi est pratique. Mais n'oubliez pas que des intrus peuvent profiter d'un wifi mal sécurisé pour intercepter facilement vos données personnelles.

QUELQUES RÉGLES FONDAMENTALES

- Assurez-vous que votre ordinateur est protégé par un logiciel antimalware.
- N'utilisez jamais des réseaux wifi publics ou hotspots connus. Hôtels, aéroports et autres lieux similaires offrent généralement des accès sécurisés, mais un peu de méfiance bien placée n'est jamais superflue. Urbizone en Région bruxelloise est sécurisé.
- Restez conscients des risques qu'implique l'envoi de données personnelles ou confidentielles (en particulier des e-mails confidentiels, des opérations financières, etc.) par le biais d'une connexion wifi.
- Ne laissez pas des clients, des fournisseurs ou d'autres personnes accéder à votre réseau wifi d'entreprise si celui-ci est connecté à votre réseau interne.

6. SMARTPHONE OU TABLETTE : PRUDENCE !

Utiliser son mobile personnel pour un usage professionnel, c'est moderne et facile, mais veillez quand même à ce que vos données professionnelles soient le plus sécurisées possible. Ces petits appareils sont facilement laissés sans surveillance : un moment de distraction et il disparaît.

QUELQUES RÉGLES FONDAMENTALES

- Évitez de mémoriser votre code pin dans la configuration de votre mobile.
- Outre votre code pin, utilisez aussi un mot de passe pour protéger l'accès à votre appareil. Réglez votre appareil pour qu'il se verrouille automatiquement après quelques secondes d'inutilisation.
- Si possible, veillez à protéger votre mobile par un logiciel antimalware.
- 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. Elles peuvent aussi contenir des logiciels espions (spyware).
- Effectuez des sauvegardes régulières sur un support externe. Vous pourriez avoir besoin de ces données pour restaurer votre appareil dans son état initial.

7. PROTÉGER SES DONNÉES LORS DE SES DÉPLACEMENTS

L'emploi d'ordinateurs portables, de smartphones ou de tablettes facilite les déplacements professionnels ainsi que l'échange de données. Ces appareils comportent cependant des risques pour les informations sensibles qui s'y trouvent, par exemple en cas de perte ou de vol.

QUELQUES RÉGLES FONDAMENTALES...

...avant de partir

- Emportez uniquement les appareils (portable, smartphone, tablette) dont vous avez besoin.
- Assurez-vous que vos appareils contiennent uniquement les informations strictement nécessaires.
- Protégez-les par un bon antimalware.
- Effectuez une sauvegarde de vos données. Vous en aurez besoin en cas de perte.
- Choisissez un mot de passe difficile à deviner et veillez à ce qu'il ne soit pas pré-enregistré (voir conseil 1)

...pendant le déplacement

- Ne perdez jamais de vue votre appareil.
- N'activez le wifi et le Bluetooth que lorsque vous en avez besoin.
- Avertissez immédiatement votre organisation en cas de perte ou de vol.
- Faites immédiatement bloquer votre carte SIM en cas de perte ou de vol.
- Informez immédiatement votre organisation en cas d'inspection ou de saisie de votre appareil par des autorités étrangères.

- Évitez de connecter votre appareil à des postes qui ne sont pas de confiance.
- N'utilisez pas votre propre clé USB ou carte mémoire si vous devez échanger des données ou les utiliser sur un autre appareil. Supprimez ensuite les données avec un programme d'effacement sûr.
- Refusez la connexion d'appareils appartenant à des tiers à votre propre appareil (smartphone, clé USB…).

…à votre retour

- Effacez les mots de passe que vous avez utilisés pendant votre déplacement.
- En cas de doute, faites vérifier votre appareil après un déplacement professionnel.
- N'utilisez jamais des clés USB que vous avez trouvées ou même qui vous ont été offertes par des inconnus (lors d'un salon, dans une réunion…).

8. UTILISER SA MESSAGERIE EN TOUTE SÉCURITÉ

Les courriels et leurs pièces jointes jouent souvent un rôle central dans les attaques informatiques (courriels frauduleux, pièces jointes piégées...).

QUELQUES RÉGLES FONDAMENTALES

- Veillez à ce que votre logiciel de messagerie soit automatiquement protégé par un logiciel antimalware.
- l'identité d'un expéditeur n'étant en rien garantie : vérifiez si le contenu d'un message est clairement en relation avec l'expéditeur supposé. En cas de doute, n'hésitez pas à contacter directement l'émetteur du mail par téléphone.
- Méfiez-vous de toutes les pièces jointes à un message et n'ouvrez aucune pièce jointe suspecte, surtout venant d'un expéditeur inconnu. Dans tous les cas, désactivez l'ouverture automatique de tels fichiers !
- Si un message contient des liens, vérifiez si l'adresse associée à ces liens correspond avec le lien lui-même. Généralement, vous pouvez le vérifier en passant la souris sur le lien sans cliquer dessus. Vous pouvez ainsi en vérifier la cohérence. Ne cliquez donc pas sans réfléchir sur chaque lien qui vous est envoyé. C'est la façon la plus classique d'injecter un virus sur votre ordinateur.
- Ne répondez jamais à un courriel qui vous demande des informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). Les entreprises de confiance telles que les banques et les fournisseurs d'accès ne le font jamais ! Il s'agit ici d'attaques par «phishing», qui n'ont pour but que de vous soutirer des informations. Supprimez immédiatement de tels messages !

9. TÉLÉCHARGER SANS SOUCIS

Si vous téléchargez des fichiers de sites web douteux, vous courez un grand risque d'installer sur votre PC des programmes illégaux ou infectés, contenant des virus ou des chevaux de Troie. Des personnes mal intentionnées pourraient ainsi prendre le contrôle à distance de votre ordinateur, voler vos données personnelles, etc.

QUELQUES RÉGLES FONDAMENTALES

- Ne téléchargez qu'à partir de sites web officiels ou fiables.
- Pensez à décocher ou désactiver toutes les options proposant d'installer des logiciels.
- Désactivez l'ouverture automatique des fichiers téléchargés.
- Veillez à ce que les fichiers téléchargés soient toujours automatiquement contrôlés par un logiciel antimalware avant leur ouverture.

10. ÊTRE VIGILANT LORS D'UN ACHAT EN LIGNE

Lorsque vous achetez en ligne, il existe un risque que vos données bancaires soient interceptées par des cybercriminels. Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site de vente.

QUELQUES RÉGLES FONDAMENTALES

- Assurez-vous que la mention « https:// » apparaît au début de l'adresse internet du site ; celle-ci identifie un environnement web sécurisé.
- Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe, par exemple.
- Préférez un mode de paiement recourant à un organisme officiel. Les banques et institutions financières utilisent généralement un lecteur de cartes générant un code.
- Ne transmettez jamais le code confidentiel de votre carte bancaire.

11. SÉPARER LES USAGES PRIVÉS DES USAGES PROFESSIONNELS

Pas besoin d'être ministre pour comprendre qu'il vaut mieux séparer strictement les usages privé et professionnel de votre ordinateur portable, de votre smartphone ou de votre messagerie. L'utilisation d'appareils privés au bureau à des fins professionnelles (« Bring your own device ») peut vous faciliter le travail de sorte que nombre d'entreprises le permettent. Vous tenez à ce que vos données privées restent confidentielles ; votre organisation a la même volonté quand il s'agit des siennes. Les causes d'une fuite de données sont le plus souvent humaines, intentionnellement ou par erreur.

QUELQUES RÉGLES FONDAMENTALES

- De préférence, séparez strictement les usages personnels des usages professionnels.
- Ne faites pas suivre vos messages électroniques professionnels sur votre messagerie personnelle.
- N'hébergez pas de données professionnelles sur vos appareils mobiles personnels ou sur des systèmes de stockage en ligne personnels.
- N'utilisez pas de supports amovibles personnels (clés USB, disques durs externes, etc.) au sein de votre organisation.

12. SURVEILLER SON IDENTITÉ NUMÉRIQUE

Sachez que pendant votre navigation sur Internet, vous laissez de nombreuses traces derrière vous. Les personnes mal intentionnées sont toujours à la recherche d'informations personnelles pour en tirer un profit financier ou vous voler votre identité. Elles tentent de trouver vos mots de passe pour accéder à vos données et pouvoir les utiliser à mauvais escient.

QUELQUES RÉGLES FONDAMENTALES

- Sur un site web ou dans un formulaire, n'entrez que les données strictement nécessaires. Les données obligatoires sont souvent clairement indiquées.
- Évitez de donner à un site web l'autorisation d'enregistrer ou de partager vos données.
- Publiez aussi peu de données privées ou professionnelles que possible sur les réseaux sociaux. Les réseaux sociaux tels que Facebook n'hésitent pas à contourner la législation nationale qui tente de vous protéger.
- Communiquez aussi peu de données privées ou professionnelles que possible dans vos discussions.
- Vérifiez régulièrement vos paramètres de sécurité et de confidentialité sur les réseaux sociaux.
- Utilisez le moins possible vos adresses mail privées et professionnelles officielles sur des sites web, hormis ceux dont vous savez qu'ils sont fiables. En cas de doute, utilisez un pseudo ou une adresse mail alternative ; vous éviterez sans aucun doute bien du spam.

13. NOTES PERSONNELLES

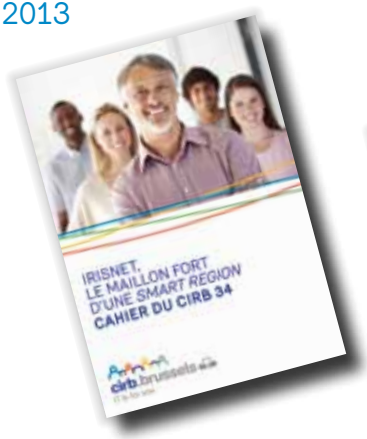
LES CAHIERS DU CIRB

Le Centre d'Informatique pour la Région Bruxelloise a pour rôle d'organiser, promouvoir et disséminer l'usage des TIC auprès des autorités et administrations locales de la Région de Bruxelles-Capitale.

Le Centre poursuit à cet effet une mission d'information, notamment par la publication de Cahiers faisant le point sur ses activités, ses projets ou encore sur l'évolution des technologies.

PUBLICATIONS RÉCENTES

2013



2014

2015

Les Cahiers du CIRB sont disponibles sous format électronique, à télécharger depuis son site Internet cirb.brussels. Pour toute information sur les Cahiers du CIRB, écrire à communication@cirb.brussels

Rédaction et coordination : Service Communication du CIRB
Imprimé avec de l'encre végétale sur papier issu de forêts gérées durablement (label FSC).

cirb.brussels
IT is for you

Editeur responsable : Hervé Feuillien
CIRB Avenue des Arts, 21 - 1000 Bruxelles
T 32 2 282 47 70 F 32 2 230 31 07
cirb.brussels - communication@cirb.brussels
@CIRB_CIBG