RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SÉCURITÉ NUMÉRIQUE

BONNES PRATIQUES À L'USAGE DES DIRECTEURS ET DES DIRECTRICES DE CAMPAGNE

SOMMAIRE

AVANT-PROPOS

Vous avez pour mission d'organiser une campagne électorale, de soutenir vos candidates et vos candidats et de mobiliser en leur faveur. Ceci nécessite de rendre visible les actions de l'équipe de campagne et vous conduit également à traiter d'informations sensibles, le plus souvent sous forme numérique.

L'usage des technologies numériques n'est pas sans risque et nécessite de respecter de bonnes pratiques simples, présentées dans ce guide.

Appliquer ces mesures permet de se prémunir de cyberattaques souvent préjudiciables aux candidates et aux candidats et à leur entourage.

Pour toute question ou précision sur ces sujets vous trouverez également de nombreuses ressources complémentaires sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : **www.ssi.gouv.fr.**

ÇA POURRAIT VOUS ARRIVER… *

SCÉNARIO 1

Par confort, une directrice de campagne choisit pour mot de passe sa date de naissance – 06101980 – et décide de l'appliquer à la majorité de ses outils numériques (messagerie, réseaux sociaux, etc.). À partir de la date de naissance figurant sur le profil de réseau social de la directrice de campagne, un attaquant retrouve le mot de passe et accède aux messages professionnels et personnels de cette dernière.

[Bonnes pratiques correspondantes : 1 - 3 - 7]

SCÉNARIO 2

Un membre de l'équipe de campagne se connecte depuis le réseau non maîtrisé d'un hôtel pour consulter sa messagerie personnelle sur laquelle il a fait suivre plusieurs messages que lui a adressés sa candidate à propos de la stratégie de campagne. Derrière le réseau qu'il croit être celui de l'hôtel se cache en réalité un attaquant qui, ayant récupéré son mot de passe de messagerie, peut désormais consulter à sa guise tous les messages reçus ainsi que les documents partagés.

[1 - 6 - 8]

SCÉNARIO 3

À l'occasion d'une conférence, un conseiller se voit offrir une clé USB qu'il connecte à son ordinateur professionnel. Cette clé contenant un rançongiciel, les données stockées sur son poste sont chiffrées et par conséquent rendues inaccessibles. Il se voit demander le paiement d'une rançon contre leur restitution. Il n'a cependant aucune garantie que le versement de la somme demandée lui permette de récupérer les informations perdues.

[2 - 5]

SCÉNARIO 4

Un directeur de campagne se fait voler son ordinateur professionnel dans le coffre de sa voiture. Pris par le temps, il n'a pas sauvegardé ses données, qui sont désormais perdues. Le mot de passe de son ordinateur : « moncandidat2022 » permet rapidement à l'attaquant d'accéder à ses fichiers, dont l'application contenant l'ensemble des données personnelles des militants du parti. Dès le lendemain, les informations volées sont publiées et l'incident fuite dans la presse, avant d'être rapidement repris sur les réseaux sociaux.

[2 - 3 - 4]

SCÉNARIO 5

Assistant à une réunion très sensible de l'équipe de campagne, une de ses membres décide de garder sur elle son téléphone, faisant fi des consignes exigeant le dépôt de ses équipements à l'extérieur de la salle.

Compromis par des attaquants, son smartphone aura permis à un groupe aux intérêts douteux de suivre la réunion en direct.

[4 - 8 - 10]

SCÉNARIO 6

Soucieux d'adresser dans les temps à son candidat des éléments préparatoires en vue d'un débat électoral, un conseiller décide de poursuivre la constitution de son dossier depuis son domicile en utilisant son ordinateur personnel. Celui-ci étant compromis, un attaquant intercepte les éléments préparés et les publie sur Internet. Les informations ainsi que l'incident sont alors largement commentés dans les médias et sur les réseaux sociaux.

[1 - 6 - 7]

---

* Toute ressemblance avec des faits réels ne serait que pure et fortuite coïncidence.

LES DIX RÈGLES D'OR

1

Séparez strictement vos usages à caractère privé de ceux liés à la campagne électorale. N'utilisez pas vos moyens de communication personnels pour vos échanges professionnels (courriel, compte d'échange de fichiers, etc.) et inversement.

2

Sauvegardez régulièrement vos données.

3

Protégez vos accès par des mots de passe correctement choisis. Ils doivent être longs et complexes, différents de vos mots de passe privés et rester secrets.

4

Ne laissez pas vos équipements sans surveillance lors de vos déplacements.

5

Protégez votre espace de travail. Verrouillez votre ordinateur lorsque vous n'êtes pas dans votre bureau.

6

Protégez votre messagerie professionnelle. Soyez vigilant avant d'ouvrir les pièces jointes et ne cliquez pas sur les liens présents dans les messages qui vous semblent douteux.

7

Préservez votre identité numérique en vous montrant vigilant sur Internet et les réseaux sociaux.

8

Évitez de connecter vos équipements sur des réseaux non maîtrisés (réseaux Wi-Fi publics, bornes de recharge USB, etc.), sauf après avis de votre équipe informatique.

9

Faites preuve de vigilance lors de vos échanges téléphoniques ou en visioconférence. La confidentialité des conversations n'est pas assurée sur les réseaux publics.

10

Veillez à la sécurité de votre smartphone, il concentre beaucoup d'informations sur votre vie numérique.

BONNES PRATIQUES

1

SÉPAREZ STRICTEMENT VOS USAGES À CARACTÈRE PRIVÉ DE CEUX LIÉS À LA CAMPAGNE ÉLECTORALE

Tous les appareils connectés sont susceptibles d'être la cible d'attaquants. Ainsi, naviguer sur Internet peut présenter des risques pour la sécurité des informations sensibles ou des données à caractère personnel que vous traitez.

- N'utilisez pas vos moyens privés (adresse électronique, clé USB, etc.) à des fins professionnelles et inversement.
- **N'utilisez jamais votre adresse électronique professionnelle pour vous inscrire sur des sites Internet** à titre privé et réciproquement.
- **Il est fortement recommandé de stocker vos données sur des espaces de stockage dédiés, maîtrisés par votre organisation.** En particulier, il est déconseillé d'utiliser les services grand public de transfert de fichiers volumineux, de stockage ou de partage disponibles sur l'Internet.

2

SAUVEGARDEZ RÉGULIÈREMENT VOS DONNÉES

Pour assurer la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires, par exemple). Vous pourrez alors en disposer même en cas de dysfonctionnement de votre système d'exploitation ou d'attaque. Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur réservé exclusivement à cet usage que vous rangerez ensuite dans un lieu éloigné de votre ordinateur pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine.

3

PROTÉGEZ VOS ACCÈS PAR DES MOTS DE PASSE CORRECTEMENT CHOISIS

Vous êtes responsable de vos mots de passe. Vous devez donc les personnaliser **dès la première utilisation de vos équipements**. Ces mots de passe doivent être longs et complexes (notamment ne pas être un mot du dictionnaire), différents de vos mots de passe privés et gardés secrets.

Vos mots de passe sont personnels et ne doivent, en aucun cas, être communiqués à autrui. Privilégiez des phrases en tant que mot de passe plutôt qu'un mot unique.

Pour vous aider dans cette démarche, l'usage d'un gestionnaire de mot de passe est à privilégier.

4

NE LAISSEZ PAS VOS ÉQUIPEMENTS SANS SURVEILLANCE LORS DE VOS DÉPLACEMENTS

Avant le départ

Ne partez qu'avec les données et les équipements nécessaires à votre déplacement. Évitez de partir avec des données sensibles. Avant de partir, sauvegardez les données que vous emportez : vous récupérerez ainsi vos informations à votre retour en cas de disparition (perte, vol, etc.) de vos équipements.

Apposez un signe distinctif mais discret sur vos appareils et sur leur housse. **Équipez l'écran de vos équipements d'un filtre de confidentialité**, afin d'en empêcher la lecture par des personnes à proximité ou encore par d'éventuelles caméras de surveillance

En déplacement

Ne laissez pas vos équipements sans surveillance lors de vos déplacements. Gardez vos équipements et supports de stockage (clés USB, etc.) avec vous. Ne les laissez pas dans un bureau ou dans une chambre d'hôtel, même dans un coffre.

Si vous êtes contraint de vous séparer de votre téléphone, ordinateur portable ou encore tablette, éteignez-les et glissez-les dans une enveloppe inviolable, après en avoir retiré les cartes mémoire à conserver sur vous. En cas de perte, de saisie, ou de vol d'un équipement, informez-en le service informatique.

Rappelez-vous que votre téléphone peut permettre de détecter votre position même a posteriori. **Si vous ne voulez pas être géolocalisé, éteignez votre appareil**. Rappelez-vous également que vos communications peuvent être écoutées, ne communiquez pas d'information confidentielle à partir de votre téléphone mobile.

Attention aux échanges de documents avec vos correspondants. **Emportez une ou plusieurs clés USB vierges exclusivement destinées à ces échanges.**

À votre retour

Si vous avez des doutes sur la compromission de l'un de vos équipements, **prenez contact avec votre responsable informatique dès votre retour,** avant de reconnecter ou d'utiliser cet équipement pour éviter tout risque de contamination ou de perte de preuve.

5

PROTÉGEZ VOTRE ESPACE DE TRAVAIL

Votre espace de travail accueille des équipements, données et documents qu'il s'agit de protéger de toute action indiscrète ou malveillante. Pour vous en prémunir, verrouillez votre poste de travail à chacune de vos absences, même très courtes, et placez vos supports de stockage (clé USB par exemple) et documents sensibles ou classifiés dans un mobilier adapté au niveau de sensibilité de l'information à protéger.

N'utilisez pas les équipements qui vous sont offerts ou inconnus (clé USB, tablette, etc.) pour un usage professionnel avant de les avoir fait vérifier par le service informatique. Ils peuvent contenir des logiciels malveillants et infecter vos systèmes à votre insu.

6

PROTÉGEZ VOTRE MESSAGERIE PROFESSIONNELLE

N'utilisez pas votre messagerie privée à des fins professionnelles et en particulier **ne faites jamais suivre les messages électroniques professionnels** sur une messagerie personnelle. En effet, la confidentialité des informations présentes dans votre messagerie personnelle ne peut être assurée. Il est également déconseillé d'utiliser votre boîte de messagerie professionnelle à des fins personnelles.

Activez si possible l'authentification à double facteur de votre messagerie électronique (qui consiste par exemple à utiliser un code de confirmation reçu par SMS en complément de votre mot de passe).

Vérifiez les liens qui figurent dans vos courriels avant de cliquer dessus et soyez vigilant avant d'ouvrir les pièces jointes : vecteur principal d'attaque, elles peuvent véhiculer des programmes malveillants.

Ne répondez jamais à des courriels vous demandant vos identifiants, des informations personnelles ou confidentielles, mais alertez immédiatement votre responsable informatique.

Enfin, de manière générale, **soyez attentif à tout indice mettant en doute l'origine réelle d'un courriel :** incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie habituellement. **Vous devez garder en mémoire que l'identité de l'expéditeur peut être usurpée.** Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre canal, par exemple téléphonique.

7

PRÉSERVEZ VOTRE IDENTITÉ NUMÉRIQUE EN VOUS MONTRANT VIGILANT SUR INTERNET ET SUR LES RÉSEAUX SOCIAUX

Les sites Internet et les réseaux sociaux sont fréquemment utilisés par des personnes malveillantes comme vecteurs d'attaques informatiques ou comme outil pour récupérer des informations personnelles. **Prenez soin de vos informations personnelles et de votre identité numérique.** Soyez notamment vigilant à l'égard des formulaires numériques que vous êtes amené à remplir. Les données que vous laissez sur Internet, et plus particulièrement sur les réseaux sociaux, échappent à votre contrôle et peuvent être récupérées et exploitées par des tiers, même lorsque vous pensez les avoir effacées.

Les consultations de sites Internet depuis vos équipements professionnels entraînent l'enregistrement d'éléments permettant d'identifier votre organisme sur les serveurs où sont hébergés ces sites. **Il est donc important d'être vigilant quant à l'utilisation qui est faite d'Internet depuis ces équipements pour éviter tout risque d'atteinte à l'image de vos candidats ou candidates.**

8

ÉVITEZ DE CONNECTER VOS ÉQUIPEMENTS PROFESSIONNELS SUR DES RÉSEAUX NON MAÎTRISÉS, SAUF APRÈS AVIS DE VOTRE ÉQUIPE INFORMATIQUE

Assurez-vous que vos équipements nomades sont suffisamment sécurisés pour utiliser des réseaux non maîtrisés. Veillez à bien vous assurer que vous vous connectez à un réseau légitime dans les lieux où vous vous rendez.

Lorsque vous vous connectez sur un réseau non maîtrisé, utilisez systématiquement le système de communication sécurisé fourni par votre organisme (VPN).

9

FAITES PREUVE DE VIGILANCE LORS DE VOS ÉCHANGES TÉLÉPHONIQUES OU EN VISIOCONFÉRENCE

Les réseaux de téléphonie (fixe ou mobile) fournis par les opérateurs ne peuvent garantir la confidentialité des communications. Aussi, ne traitez pas de sujets à caractère sensible sur ces réseaux.

La confidentialité des échanges n'est pas non plus garantie par les applications grand public de visioconférence. Il en est de même pour les conférences effectuées depuis des équipements spécifiques.

10

VEILLEZ À LA SÉCURITÉ DE VOTRE SMARTPHONE

Soyez attentif à votre environnement lorsque vous passez un appel et évitez les appels depuis les lieux publics dans lesquels vos conversations peuvent être écoutées. Gardez à l'esprit que votre téléphone peut permettre de détecter votre position à votre insu. **Lorsque vous ne souhaitez pas être géolocalisé, éteignez votre appareil.**

Évitez de prendre votre équipement pendant les réunions au cours desquelles des sujets sensibles sont à l'ordre du jour, ou a minima, éteignez-le. En effet, ces équipements mobiles peuvent être utilisés pour enregistrer les conversations, y compris à l'insu de leur propriétaire.

Protégez l'accès à votre smartphone par un code secret et configurez-le pour qu'il se verrouille automatiquement. **Soyez prudent avec les applications que vous installez** et vérifiez les autorisations qu'elles nécessitent avant de les télécharger (accès à vos informations géographiques, à vos contacts, au journal des appels téléphoniques, etc.).

RÉAGIR EN CAS DE CYBERATTAQUE

- **N'éteignez pas les équipements piratés mais déconnectez-les immédiatement du réseau** afin d'éviter la propagation de l'attaque et de préserver les preuves nécessaires à l'enquête.
- **Ne connectez plus aucun appareil sur le réseau.**
- **Contactez immédiatement votre service informatique.** Le responsable informatique doit être clairement identifié par tous (et ses coordonnées connues) avant que l'incident ne se produise.
- **Portez plainte auprès des services compétents** (Police nationale ou Gendarmerie nationale). La plainte doit être déposée par un représentant légal de votre entité ou toute personne disposant d'un mandat de représentation.
- **Constituez une équipe pour gérer les conséquences de la cyberattaque et préparer une stratégie de communication.**

N'hésitez pas également à consulter le site de l'**ANSSI** :
www.ssi.gouv.fr/en-cas-dincident/

« En vue d'un débat, un conseiller décide de poursuivre la constitution de son dossier depuis son domicile. Son ordinateur personnel étant compromis, un attaquant intercepte les éléments préparés et les publie sur Internet [...] »

Extrait du scénario 6,

chapitre « Ça pourrait vous arriver... »

Version 2.0 – Octobre 2021 – **ANSSI-GP-088**

ISBN : 978-2-11-167106-5 (papier)
ISBN : 978-2-11-167107-2 (version numérique)
Dépôt légal : octobre 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr