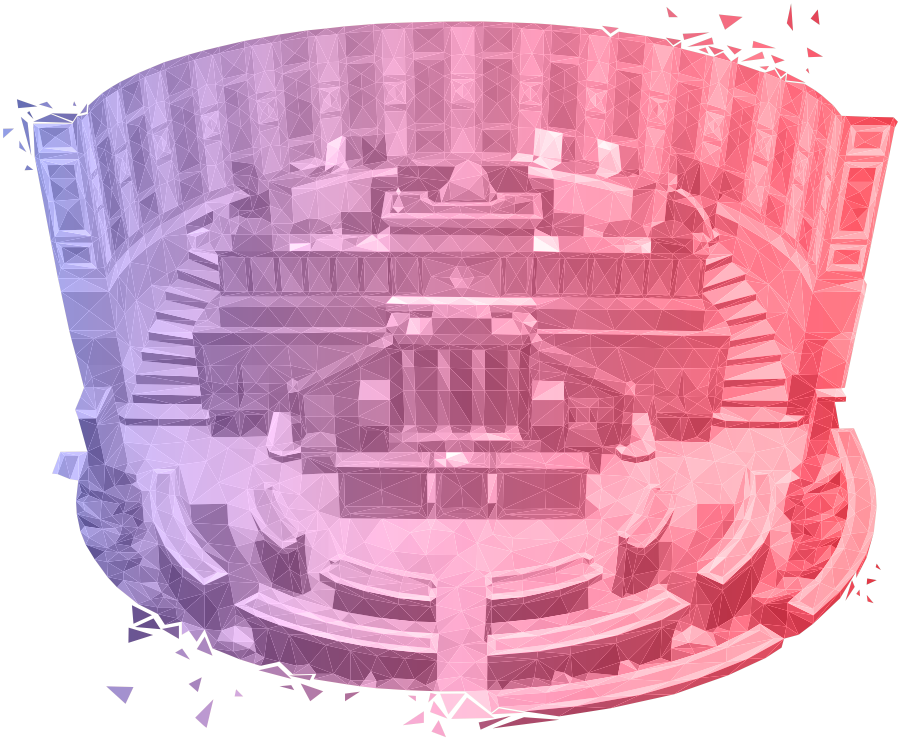
SÉCURITÉ NUMÉRIQUE

BONNES PRATIQUES À L'USAGE DES SÉNATEURS



AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

SOMMAIRE

AVANT-PROPOS

Votre mandat vous amène à traiter d'informations sensibles* souvent sous forme numérique, qui méritent à ce titre une protection particulière.

La réduction des risques induits par l'usage des technologies de l'information et de la communication repose d'abord sur le respect de bonnes pratiques simples à adopter.

Elles sont réunies dans ce guide coréalisé par la direction des systèmes d'information du Sénat et l'Agence nationale de la sécurité des systèmes d'information (ANSSI). **Appliquer ces mesures permet de se prémunir de cyberattaques souvent préjudiciables à votre image ou à celle de l'institution, à la sécurité nationale et à la compétitivité de la France.**

Pour toute question ou précision sur ces sujets, vous pouvez vous adresser au responsable de la sécurité des systèmes d'information du Sénat (voir la page contact à la fin de ce guide).

Vous trouverez également des informations complémentaires sur le site de l'ANSSI : www.ssi.gouv.fr.

---

* *Affaires économiques, sujets relevant du secret de la défense nationale, relations internationales, etc.*

ÇA POURRAIT VOUS ARRIVER... *

SCÉNARIO 1

Par commodité, un sénateur choisit pour mot de passe ses initiales suivies de sa date de naissance – IJ06101980 – et décide de l'appliquer à la plupart de ses équipements (téléphone mobile, tablette, etc.). À partir de la date de naissance figurant sur son profil de réseau social, un attaquant retrouve le mot de passe et accède aux messages professionnels et personnels de ce dernier.

[Numéros des bonnes pratiques correspondantes : **1 – 2 – 3 - 7**]

SCÉNARIO 2

Une députée se connecte depuis le réseau non maîtrisé d'un hôtel pour consulter sa messagerie personnelle sur laquelle elle a fait suivre plusieurs messages concernant les affaires en cours de sa circonscription. Derrière le réseau qu'elle croit être celui de l'hôtel se cache en réalité un attaquant qui, ayant récupéré son mot de passe de messagerie personnelle, peut désormais consulter à sa guise les informations professionnelles accessibles.

[1 - 6 - 8]

SCÉNARIO 3

À l'occasion d'une conférence du G20, un conseiller ministériel se voit offrir une clé USB qu'il connecte immédiatement à son ordinateur professionnel. Cette clé portant un programme malveillant de type rançongiciel, les données stockées sur son poste sont chiffrées et par conséquent rendues inaccessibles. Seul le paiement d'une rançon peut permettre au conseiller de les récupérer, mais le versement de la somme demandée ne garantit pas leur restitution.

[5]

SCÉNARIO 4

Un agent ministériel se fait voler son ordinateur personnel dans le coffre de sa voiture. Interrogé, il signale aux autorités qu'il y stockait un répertoire contenant l'ensemble de ses contacts interministériels. Dès le lendemain, l'incident fuite dans la presse et est rapidement repris sur les réseaux sociaux.

[1 - 2 - 4]

SCÉNARIO 5

Dans le cadre d'un groupe d'amitié, un député en déplacement à l'étranger égare dans un taxi la sacoche contenant son ordinateur et son téléphone professionnels. Préoccupé par les préparatifs du départ, il n'a pas sauvegardé les données qui s'y trouvent. Elles sont désormais perdues et susceptibles de tomber entre de mauvaises mains.

[4]

SCÉNARIO 6

Dans le cadre d'une audition lors d'une commission, rassuré par l'activation d'un brouilleur, un sénateur décide de garder son téléphone allumé. Compromis, le téléphone a permis à un groupe aux intérêts douteux d'accéder à l'enregistrement a posteriori de cette réunion.

[2 - 4 - 8]

SCÉNARIO 7

Soucieux d'adresser dans les temps son dossier à un partenaire, un agent de l'État décide de poursuivre la constitution de ce dossier sensible depuis son domicile en utilisant les moyens personnels à sa disposition. Son ordinateur personnel étant compromis, un attaquant intercepte le dossier et fait échouer le projet en faisant fuiter dans la presse les données transmises.

[1 – 2 - 6 - 7]

---

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

LES DIX

1

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

2

Soyez vigilant lors de l'utilisation de vos outils informatiques, notamment lors de vos déplacements. Conservez votre sens critique.

3

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

4

En déplacement, protégez vos données et ne laissez pas vos équipements sans surveillance.

5

Protégez votre espace de travail. Verrouillez votre poste de travail lorsque vous n'êtes pas dans votre bureau. Maintenez vos équipements et applications à jour.

RÈGLES D'OR

6

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

8

Connectez vos équipements sur des réseaux maîtrisés.

7

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

9

Faites preuve de vigilance lors de vos échanges téléphoniques ou en visioconférence. La confidentialité des conversions 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 personnel de ceux liés à votre mandat

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 que vous traitez ou celle de vos données à caractère personnel.

- N'utilisez pas vos moyens personnels (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 personnel et réciproquement.

2

Soyez vigilant lors de l'utilisation de vos outils informatiques

L'efficacité des outils que vous utilisez est conditionnée par l'emploi que vous allez en faire. Si vous avez des questions sur les services mis à votre disposition ou si vous suspectez une compromission de vos outils, **contactez la direction des systèmes d'information du Sénat.**

Certaines des informations que vous allez traiter lors de votre mandat sont sensibles ou classifiées. À ce titre, elles sont soumises à des obligations de protection particulières et doivent par conséquent être conservées et transmises via les moyens adaptés. À cet égard, **il est recommandé de ne pas utiliser les services grand public de transfert de fichiers volumineux**, de stockage ou de partage disponibles sur Internet.

Conservez votre sens critique : ne faites pas dans votre vie numérique ce que vous jugez imprudent de faire dans votre vie de tous les jours.

3

Protégez vos accès par des mots de passe correctement choisis

Vous êtes responsable de vos mots de passe. Vous devez donc les choisir **dès la première utilisation de vos équipements ou modifier immédiatement ceux qui vous sont fournis.** Ces mots de passe doivent être complexes (notamment ne pas figurer dans le dictionnaire), différents de vos mots de passe personnels, régulièrement renouvelés et gardés secrets. La fiche « Les mots de passe », disponible depuis l'option « Sécurité » du pavé « Informatique » de la page « Pratique » sur l'intranet du Sénat vous aidera à choisir un mot de passe robuste.

N'oubliez pas que vos mots de passe sont personnels et ne doivent en aucun cas être communiqués à autrui.

4

Lors de vos déplacements, protégez vos données et ne laissez pas vos équipements sans surveillance

Avant le départ

Ne partez qu'avec les données nécessaires à votre déplacement. Évitez de partir avec des données sensibles. Sauvegardez avant de partir 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 en toute circonstance 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, si possible, 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 la direction des systèmes d'information au plus tôt.

Rappelez-vous que votre téléphone peut permettre de vous géolocaliser, même a posteriori. **Si vous ne voulez pas l'être, 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. N'utilisez jamais de support de stockage offert par votre correspondant.**

À votre retour

Si vous avez des doutes sur la compromission de l'un de vos équipements ou sur l'innocuité d'un cadeau technologique, **prenez contact avec votre responsable de la sécurité des systèmes d'information 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.

Au quotidien, utilisez votre ordinateur avec un compte n'ayant pas la possibilité d'installer de nouveaux logiciels appelé « compte utilisateur ». Un second compte, dit « compte administrateur », doit être installé pour permettre d'intervenir facilement sur le fonctionnement global de l'ordinateur. **Téléchargez vos programmes sur les sites des éditeurs**, ou d'autres sites de confiance.

Réalisez des sauvegardes régulières de vos données sur un support amovible spécifique externe (clé USB, disque dur) conservé dans un endroit protégé.

Configurez vos différents équipements pour que les mises à jour de sécurité (systèmes d'exploitation et applications) s'installent automatiquement et durcissez la configuration de votre ordinateur en utilisant des solutions de sécurité éprouvées (pare-feu[1], antivirus[2], etc.).

---

1 *Logiciel ou matériel permettant de filtrer les flux réseau de manière à n'autoriser que les flux réseau légitimes.*

2 *Logiciel destiné à identifier, neutraliser et effacer des logiciels malveillants.*

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 la direction des systèmes d'information. Ils peuvent contenir des logiciels malveillants et infecter vos systèmes à votre insu.

N'utilisez jamais vos équipements pour recharger votre smartphone ou celui d'autrui.

6

Protégez votre messagerie professionnelle

N'utilisez pas votre messagerie personnelle à des fins professionnelles et en particulier **ne faites jamais suivre de manière automatique 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 boite de messagerie professionnelle à des fins personnelles. **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 ou des informations personnelles, mais alertez immédiatement votre responsable de la sécurité des systèmes d'information.

N'envoyez jamais de fichiers sensibles sur Internet sans les avoir préalablement protégés.

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.** Si vous avez des doutes, **prenez contact avec votre responsable de la sécurité des systèmes d'information.**

7

Préservez votre identité numérique en vous montrant vigilant sur Internet et 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, vous échappent de manière irréversible.

Les consultations de sites Internet depuis le Sénat 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 vos équipements pour éviter tout risque d'atteinte à votre image et à celle du Sénat.**

8

Connectez vos équipements sur des réseaux maîtrisés

Assurez-vous que les réseaux sur lesquels vous connectez vos équipements nomades sont suffisamment sécurisés. À cet égard, il est recommandé de ne pas utiliser de réseaux Wi-Fi ouverts (sans mots de passe requis) et de privilégier les réseaux maîtrisés par l'organisme qui vous accueille en vous faisant confirmer le nom et le moyen d'authentification associé.

Il est également recommandé de ne pas utiliser les bornes de recharge USB mises à disposition dans les lieux publics (aéroports, trains, hôtels, etc.). Elles peuvent être piégées pour infecter vos équipements.

9

Faites preuve de vigilance lors de vos échanges téléphoniques ou en visioconférence

Les réseaux de téléphonie fournis par les opérateurs ne peuvent garantir la confidentialité des communications. Aussi, ne traitez pas de sujet sensible sur ces réseaux.

La confidentialité des échanges n'est pas non plus garantie par les applications grand public de visioconférence disponibles sur ordinateurs et tablettes. 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 vous géolocaliser à votre insu. **Lorsque vous ne souhaitez pas l'être, éteignez votre appareil.**

Éteignez votre équipement pendant les réunions au cours desquelles des sujets sensibles sont à l'ordre du jour. 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 ou à votre tablette 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 données géographiques, à vos contacts, à l'historique de vos appels téléphoniques, etc.).

Quand cela est possible, activez les fonctions de sécurité disponibles sur votre appareil (chiffrement, interdire les applications de sources inconnues, etc.).

Informations pratiques

Support informatique

Tél : 20 70
Mél : 2070@senat.fr

Responsable de la sécurité des systèmes d'information

Tél : 34 59
Mél : rssi@senat.fr

Intranet du Sénat

https://intra.senat.fr/

Les pages de la direction des systèmes d'information

https://intra.senat.fr/group/senat/systemes-d-information/accueil

Pour consulter :

- la charte d'usage des moyens informatiques ;
- la méthode pour construire des mots de passe robustes (mais faciles à retenir) ;
- les pas à pas informatiques (en particulier comment changer son mot de passe annuaire).

Site de l'ANSSI
http://www.ssi.gouv.fr

NOTES

SÉCURITÉ NUMÉRIQUE

BONNES PRATIQUES À L'USAGE DES SÉNATEURS

[…] rassuré par l'activation d'un brouilleur, un sénateur décide de garder son téléphone allumé. Compromis, le téléphone a permis à un groupe aux intérêts douteux […]

Extrait du scénario 6,
chapitre *Ça pourrait vous arriver...*

Version 1.0 – Novembre 2017
20171116-1601

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN