université PARIS-SACLAY

LUTTER CONTRE LA CYBERMALVEILLANCE

KIT DE SENSIBILISATION

LUTTER CONTRE LA CYBERMALVEILLANCE

La multiplication et la diversification des cybermenaces en font un phénomène complexe à appréhender pour les particuliers et/ou collaborateurs. « De quoi s'agit-il exactement ? », « Quels sont les risques ? », « Suis-je concerné ? » et « Comment me prémunir ? » : autant de questions auxquelles ce kit de sensibilisation qui est une adaptation de celui réalisé par Cybersurveillance.gouv.fr pour l'Université Paris-Saclay tente de répondre.

Ce kit vise à sensibiliser aux questions de sécurité numérique, à partager les bonnes pratiques dans les usages personnels, et de manière vertueuse, à améliorer les usages dans le cadre professionnel.

Ce kit de sensibilisation est composé de 9 thématiques avec des fiches pour adopter les bonnes pratiques et des fiches pour comprendre les risques.

http://www.di.universite-paris-saclay.fr/securite/docs/kit_sensibilisation_ssi.pdf

LES MOTS DE PASSE

Mémo

ADOPTER LES BONNES PRATIQUES

8 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1. Utilisez un mot de passe différent pour chaque compte
2. Utilisez un mot de passe suffisamment long et complexe
3. Utilisez un mot de passe impossible à deviner
4. Ne communiquez jamais votre mot de passe à un tiers
5. Changez votre mot de passe au moindre soupçon
6. Utilisez un gestionnaire de mot de passe
7. Activez la double authentification lorsque c'est possible
8. Changez les mots de passe par défaut des différents services auxquels vous accédez

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

LES COURRIELS

Mémo

ADOPTER LES BONNES PRATIQUES

6 CONSEILS LORSQUE VOUS RECEVEZ DES COURRIELS

1. Vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifiez son identité
2. 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
3. Si des liens figurent dans un courriel, passez la souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur S'il y a une différence, ne jamais cliquer sur le lien
4. Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (hameçonnage)
5. N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité…
6. Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

université PARIS-SACLAY

LES DONNÉES PERSONNELLES

Mémo

ADOPTER LES BONNES PRATIQUES

5 CONSEILS POUR PROTÉGER SES DONNÉES PERSONNELLES

1. Ne transmettez que les informations nécessaires et décochez les cases qui autoriseraient le site à conserver ou à partager vos données
2. Ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux et soyez vigilant lors de vos interactions avec les autres utilisateurs
3. Vérifiez régulièrement vos paramètres de sécurité et de confidentialité
4. Utilisez plusieurs adresses électroniques dédiées aux différentes activités sur Internet
5. Limitez au maximum la diffusion de données personnelles de vos contacts professionnels internes ou externes à l'université

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
dpd@universite-paris-saclay.fr
securite.di@universite-paris-saclay.fr

LES USAGES PRO-PERSO

Mémo

ADOPTER LES BONNES PRATIQUES

10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

1. Utilisez des mots de passe différents pour tous les comptes professionnels et personnels auxquels vous accédez
2. Ne mélangez pas votre messagerie professionnelle et personnelle
3. Ayez une utilisation raisonnable d'Internet au travail
4. Maîtrisez vos propos sur les réseaux sociaux
5. N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles
6. Faites les mises à jour de sécurité de vos équipements
7. Utilisez une solution de sécurité contre les virus et autres attaques
8. N'installez des applications que depuis des sites ou magasins officiels
9. Méfiez-vous des supports USB
10. Évitez les réseaux Wi-Fi publics ou inconnus

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

université PARIS-SACLAY

L'HAMEÇONNAGE *(filoutage ou phishing)*

COMPRENDRE LES RISQUES

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue ou d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (filoutage ou *phishing,* en anglais)

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux

TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

COMMENT RÉAGIR ?

- Ne communiquez jamais d'informations sensibles suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement en cas d'arnaque bancaire
- Changez vos mots de passe divulgués / compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir liens utiles)

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

LIENS UTILES :
Signalspam.fr Phishing-initiative.fr
Info escroqueries : 0 805 805 817 (gratuit)

LES RANÇONGICIELS *(ransomware)*

COMPRENDRE LES RISQUES

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ?
Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais)

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système

COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- Dans l'établissement, alertez votre service informatique et le pôle Sécurité de la DSI (Direction des Systèmes d'information) : securite.di@universite-paris-saclay.fr
- Ne payez pas la rançon
- Faites-vous assister par des professionnels

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

LIEN UTILE :
www.nomoreransom.org/fr/index.html

université PARIS-SACLAY

LES RÉSEAUX SOCIAUX

Mémo

ADOPTER LES BONNES PRATIQUES

10 CONSEILS POUR VOTRE SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

1. Protégez l'accès à votre compte
2. Vérifiez les paramètres de confidentialité
3. Maîtrisez vos publications
4. Faites attention à qui vous parlez
5. Changez votre mot de passe au moindre soupçon
6. Évitez les ordinateurs et les réseaux Wi-Fi publics
7. Vérifiez régulièrement les connexions à votre compte
8. Faites preuve de discernement avec les informations publiées
9. Utilisez en conscience l'authentification avec votre compte de réseau social sur d'autres sites
10. Supprimez votre compte si vous ne l'utilisez plus

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

LES APPAREILS MOBILES

Mémo

ADOPTER LES BONNES PRATIQUES

9 CONSEILS POUR SÉCURISER VOTRE APPAREIL MOBILE PRO

1. Mettez en place les codes d'accès
2. Appliquez les mises à jour de sécurité
3. Faites des sauvegardes
4. Utilisez une solution de sécurité contre les virus et autres attaques
5. N'installez des applications que depuis les sites ou magasins officiels
6. Contrôlez les autorisations de vos applications
7. Ne laissez pas votre appareil sans surveillance
8. Évitez les ordinateurs et les réseaux Wi-Fi publics
9. Ne stockez pas d'informations confidentielles sans protection

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

université PARIS-SACLAY

LES DÉPLACEMENTS (1)

Mémo

ADOPTER LES BONNES PRATIQUES

16 CONSEILS LORSQUE VOUS PARTEZ EN MISSION

AVANT LA MISSION

1. N'utilisez que du matériel dédié à la mission et ne contenant que les données nécessaires
2. Sauvegardez ces données pour les retrouver en cas de perte
3. Utilisez un filtre de protection-écran pour votre ordinateur
4. Apposez un signe distinctif sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport
5. Vérifiez que vos mots de passe ne sont pas préenregistrés

PENDANT LA MISSION

6. Gardez vos appareils, supports papiers avec vous, pendant votre voyage, séjour
7. Désactivez les fonctions Wi-Fi et Bluetooth de vos appareils
8. Retirez la carte SIM et la batterie (dans la mesure du possible) si vous êtes contraint de vous séparer de votre téléphone
9. Informez l'établissement en cas d'inspection ou de saisie de votre matériel par des autorités étrangères
10. N'utilisez pas les équipements que l'on vous offre
11. Évitez de connecter vos équipements à des postes qui ne sont pas de confiance
12. Refusez la connexion d'équipements appartenant à des tiers à vos propres équipements

LES DÉPLACEMENTS (2)

Mémo

ADOPTER LES BONNES PRATIQUES

16 CONSEILS LORSQUE VOUS PARTEZ EN MISSION

APRÈS LA MISSION

13. Effacez l'historique des appels et de navigation
14. Changez les mots de passe que vous avez utilisés pendant le voyage
15. Faites analyser vos équipements après la mission, si vous le pouvez
16. N'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements : elles sont susceptibles de contenir des programmes malveillants

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr
securite.prevention@universite-paris-saclay.fr

université PARIS-SACLAY

UN PEU DE VOCABULAIRE

VOCABULAIRE

A

ANSSI : L'Agence Nationale de la Sécurité des Systèmes d'Information est l'autorité en matière de sécurité et de défense des systèmes d'information de l'État

B

Botnet : Réseaux d'ordinateurs ou de sites internet compromis par un attaquant et utilisé par exemple à des fins de diffusion de courriels non désirés, ou d'attaques informatiques

C

Code malveillant : Virus, Ver… Programmes informatiques dont la fonction est de détourner l'ordinateur de son usage légitime.
Cryptage (ou chiffrage) : Destiné à sécuriser les informations. Ce principe transforme les messages en chiffres, afin de les rendre incompréhensibles à toutes les personnes à qui les informations ne sont pas destinées.

D

Déni de service ou DDoS : Attaque par dénis de service. Attaque informatique visant à rendre inaccessible une ressource internet par l'envoi de multiples requêtes de connexion, par le biais de botnets.
Défaçage : Défacement ou défiguration désigne la modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site. Il s'agit d'une forme de détournement de site web par un hacker.
DPD (ou *DPO*) : Délégué à la Protection des Données ou *Data Protection Officer* est la personne chargée de la protection des données personnelles au sein d'une organisation.

F

Faille : Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.
FSD : Le Fonctionnaire Sécurité Défense a, dans les établissements publics d'enseignement supérieur et de recherche, pour mission de mettre en application les plans de défense et de protéger le potentiel scientifique et technique par la mise en œuvre des dispositifs de prévention et de protection des intérêts fondamentaux de la nation, que constituent notamment les résultats de la recherche scientifique..

UN PEU DE VOCABULAIRE

VOCABULAIRE

H

Hameçonnage / Filoutage (ou *Phishing*) : Techniques utilisées pour obtenir frauduleusement des informations personnelles. La victime est invitée à cliquer sur un lien avec la certitude qu'elle arrive sur un site connu et digne de confiance, puis il lui est proposé de vérifier quelques informations. Si celle-ci fournit les informations, alors le phishing est réussi.

P

Pare-feu (ou *Firewall*) : Logiciel permettant de protéger les données d'un ordinateur ou réseau. Il filtre les entrées et contrôle les sorties, selon des règles définies par son administrateur.
PSSI-E : Politique de Sécurité des Systèmes d'Information de l'État. C'est un document qui fixe les règles de protection applicables aux systèmes d'information de l'État.
PSST : La Protection du Potentiel Scientifique et Technique de la nation a pour but de protéger, au sein des établissements publics et privés, l'accès à leurs savoirs et savoir -faire stratégiques ainsi qu'à leurs technologies sensibles. Elle permet de se prémunir plus efficacement contre les tentatives de captation d'informations et de techniques.

R

Rançongiciel (ou *Ransomware*) : Logiciel malveillant qui rend invisibles les données en les chiffrant. Une demande de rançon est alors envoyée, la victime devra donc payer pour récupérer ses données qui seront à nouveau visibles.
RGPD : Règlement Général sur la Protection des Données. Règlement européen modifiant le cadre juridique relatif à la protection des données personnelles.
RSSI : Responsable de la Sécurité des Systèmes d'Information est l'expert qui garantit la sécurité, la disponibilité et l'intégrité du système d'information et des données dans son établissement.

S

SSI : Sécurité des Systèmes d'Information. Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées.

université PARIS-SACLAY

LIENS UTILES

LIENS UTILES

SECURITE DSI :
http://www.di.universite-paris-saclay.fr/securite/
ANSSI :
https://www.ssi.gouv.fr/
CYBERMALVEILLANCE :
https://www.cybermalveillance.gouv.fr/
PHISHING :
https://phishing-initiative.fr/contrib/
https://www.phishtank.com/
https://safebrowsing.google.com/safebrowsing/report_phish/?hl=fr
RANSOMWARE :
https://www.nomoreransom.org/fr/index.html

DOCUMENTATION

Guide des bonnes pratiques de l'ANSSI :
https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
Kit de sensibilisation du site cybermalveillance :
https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/
PSSI-E :
https://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf
MOOC ANSSI :
https://www.secnumacademie.gouv.fr/
Abécédaire de la cybersécurité :
https://www.usinenouvelle.com/expo/guides-d-achat/l-abecedaire-de-la-cyber-securite-179

CONTACTS

CONTACTS

PÔLE SÉCURITÉ – DSI – UNIVERSITÉ PARIS-SACLAY
securite.di@universite-paris-saclay.fr

RSSI – UNIVERSITÉ PARIS-SACLAY
rssi@universite-paris-saclay.fr

DPD – UNIVERSITÉ PARIS-SACLAY
dpd@universite-paris-saclay.fr

FSD – UNIVERSITÉ PARIS-SACLAY
securite.prevention@universite-paris-saclay.fr

EN CAS DE PROBLÈME, VEUILLEZ CONTACTER :
securite.di@universite-paris-saclay.fr

université PARIS-SACLAY