Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SÉCURITÉ INFORMATIQUE

MEMENTO CYBERSECURITÉ POUR LE CONSOMMATEUR

ÊTRE CONSOMMATEUR, C'EST...

DISPOSER D'UN TERMINAL INFORMATIQUE

Accéder au monde numérique implique l'utilisation d'un terminal informatique, qu'il s'agisse d'un téléphone portable, d'une tablette, d'un ordinateur portable ou fixe. Un terminal informatique comprend des logiciels. Avec le temps, les éditeurs découvrent que ces logiciels sont vulnérables et apportent des correctifs compris dans les mises à jour. Sans ces mises à jour, des portes d'entrée sont laissées aux pirates.

METTRE À JOUR RÉGULIÈREMENT SES ÉQUIPEMENTS

Des conditions d'utilisations accompagnent certains appareils. Il convient de les respecter en évitant d'installer des logiciels non autorisés. Le respect de ces règles participe à la sécurité de vos données.

RESPECTER LES CONDITIONS D'UTILISATION DE VOS APPAREILS

Des informations confidentielles peuvent être stockées sur un équipement informatique. Afin de protéger vos documents en cas de vol ou d'accès physique à l'appareil, il convient de verrouiller son appareil par un code ou mot de passe.

VERROUILLER L'ACCÈS À SON PROFIL UTILISATEUR

Certains logiciels de traitement de texte proposent d'ajouter un code pour consulter un document. Il s'agit d'un premier niveau de sécurité. Lorsque le logiciel ne dispose pas de cette option, il est également possible de « chiffrer » le document à l'aide d'un logiciel spécifique.

VERROUILLER L'ACCÈS AUX FICHIERS CONFIDENTIELS

On ne peut prévoir tous les scénarios catastrophes et une défaillance matérielle peut toujours arriver. Pour éviter de perdre ses documents définitivement en cas d'incident, une sauvegarde régulière est nécessaire.

SAUVEGARDER RÉGULIÈREMENT SES FICHIERS

Pour aller plus loin :
https://www.internet-signalement.gouv.fr/PortailWeb/planets/Conseils.action

...SE RENDRE SUR DES SITES MARCHANDS

Il existe deux types de sites internet. Ceux dont l'adresse commence par http:// qui n'assurent pas la confidentialité des informations échangées, et ceux dont l'adresse commence pas https:// et qui assurent la confidentialité des informations échangées.

Il ne faut jamais accepter de créer un compte sur un site lorsque l'url commence par http:// car les informations (mot de passe, informations personnelles) peuvent être interceptées par des tiers.

NE JAMAIS PARTAGER DES INFORMATIONS PERSONNELLES (MOT DE PASSE, INFORMATIONS BANCAIRES ETC.)...

...avec des sites marchands dont l'adresse ne commence pas par https://

CONSULTER RÉGULIÈREMENT SON COMPTE BANCAIRE EN LIGNE

La technologie du « 3D secure » est un outil supplémentaire de sécurité. Il permet de valider un achat distant par un code obtenu par sms.

Pour aller plus loin :

Guide de l'acheteur en ligne :
https://www.economie.gouv.fr/files/files/directions_services/dgccrf/documentation/publications/depliants/acheteur-en-ligne.pdf

La banque à distance :
http://www.fbf.fr/fr/files/9WEJYY/Guide-securite-4.pdf

...C'EST UTILISER DES MOTS DE PASSE

Les sites marchands peuvent faire l'objet d'un incident de sécurité permettant à un tiers d'accéder aux mots de passe. Un consommateur utilisant le même mot de passe sur différents sites internet se place donc en vulnérabilité. Afin de renforcer sa sécurité numérique, il est préférable de varier les mots de passe et de réserver chacun à un usage unique.

1 COMPTE = 1 MOT DE PASSE DÉDIÉ

Pour aller plus loin :
https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

La multiplication de comptes sur différents sites marchands rend difficile la gestion de nombreux mots de passe, d'autant qu'ils doivent respecter certaines caractéristiques ce qui tend à les rendre difficiles à

mémoriser. Des logiciels existent et aident à la gestion des mots de passe.

UTILISER UN GESTIONNAIRE DE MOT DE PASSE

Pour aller plus loin :
https://www.cnil.fr/fr/atom/14984

...C'EST DISPOSER D'UNE MESSAGERIE

La messagerie électronique est un outil permettant de communiquer facilement. L'adresse électronique est le plus souvent utilisée pour créer un compte auprès d'un site marchand et l'on y reçoit factures et messages promotionnels.

C'est également un outil prisé par des personnes malveillantes pour obtenir des informations confidentielles (codes d'accès, informations bancaires etc.).

Certaines informations doivent attirer votre attention, notamment sur la crédibilité du contenu :

- Suis-je censé recevoir un tel courriel (message rédigé dans une langue étrangère, expéditeur inconnu etc.)
- Suis-je effectivement client de cet établissement ?
- L'adresse e-mail correspond-elle effectivement à l'entreprise qu'elle prétend être ?

UN COURRIEL N'EST PAS ANODIN, AYEZ UN REGARD CRITIQUE

Pour aller plus loin :

À propos du phishing
https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage

Sur les faux sites administratifs
https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/faux-sites-administratifs-attention-aux-arnaques

La levée du doute peut être réalisée :

- S'il s'agit d'une facture, puis-je y accéder par mon espace client situé sur le site internet officiel sans cliquer sur le lien contenu dans le courriel ?
- En téléphonant au service client de cette entreprise (numéro de téléphone présent sur une ancienne facture ou sur le site officiel)

...C'EST COMMUNIQUER AVEC PRÉCAUTION

Les réseaux sociaux sont des lieux d'échanges. Soyez vigilant sur l'information que vous divulguez à la vue de tous.

Demandez-vous si l'information que vous êtes sur le point de publier sur internet est confidentielle. Si cela avait été dans la vie réelle, l'auriez-vous divulguée ? D'autant que ce qui s'écrit sur la toile s'efface difficilement !

RESTEZ VIGILANT ; NE CONTRIBUEZ PAS À VOTRE PROPRE PIRATAGE.

À l'instar du phishing (hameçonnage), des demandes d'informations personnelles peuvent se faire par des interlocuteurs qui peuvent évoquer des situations d'urgence, des demandes de confirmation, etc.

Cette méthode se nourrit de notre manque d'attention. Dans ce type de contexte, il convient de s'assurer de l'identité réelle de votre interlocuteur et d'obtenir des informations pour juger de sa vraisemblance et de sa réalité.

S'ASSURER DE L'IDENTITÉ DU DEMANDEUR D'INFORMATIONS ET MIEUX ÉVALUER LA RÉALITÉ DU CONTEXTE SONT DES RÉFLEXES INDISPENSABLES

EN CAS D'INCIDENT

Si malgré vos précautions, vous êtes victime d'un incident de cybersécurité, le groupe d'intérêt public ACYMA a mis sur pied le site www.cybermalveillance.gouv.fr pour mettre en relation entreprises, prestataires spécialisés et organismes compétent proches de chez vous.

En cas d'incident
https://www.cybermalveillance.gouv.fr

Signaler un contenu illicite
https://www.internet-signalement.gouv.fr

Signaler un contenu illicite
http://www.pointdecontact.net/

SG
Secrétariat général

HFDS Bercy

Secrétariat Général
139-145 rue de Bercy, PARIS
Septembre 2017