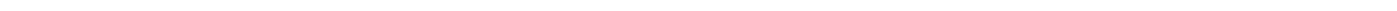


# #8 Sécurité Numérique

Publié le 2 mars 2022 – Mis à jour le 4 mars 2022













Date(s)

le 2 mars 2022

La sécurité informatique est une préoccupation majeure, encore plus en ce moment, où nous traversons plusieurs crises. Un bon comportement avec les outils informatiques est le premier rempart face à ces attaques.

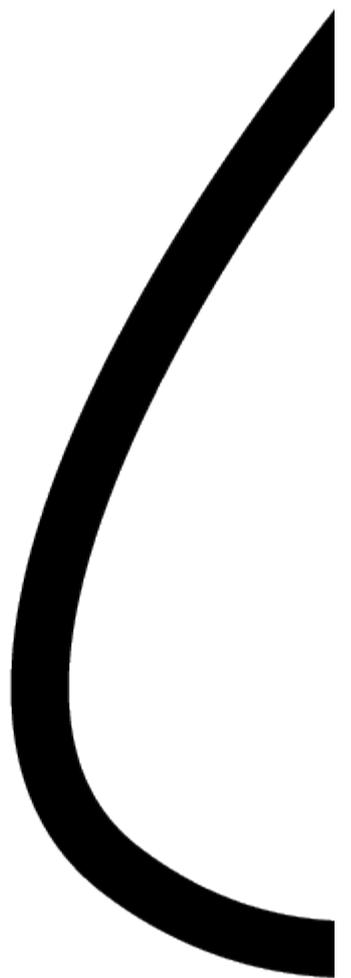
*LA PÉRIODE ACTUELLE EST PROPICE À  
UNE RECRUESCENCE DES  
CYBERATTAQUES.*

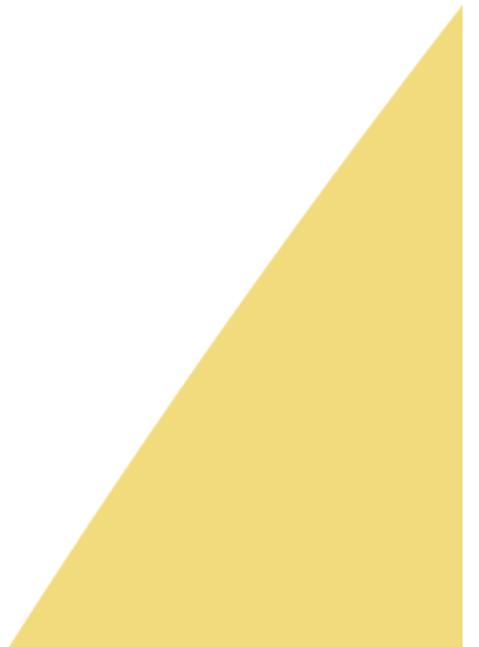
Afin de garantir la continuité de notre mission de service public, l'intégrité de notre activité et pour que nos dispositifs informatiques ne soient pas détournés pour des **attaques par rebond** vers d'autres structures, **il est impératif de protéger nos outils et nos données.**

Cette sécurité relève à la fois de **nos dispositifs techniques en amont des réseaux** mais aussi de l'**attention que chacun d'entre nous porte au respect d'un certain nombre de préconisations**, avec le plus haut degré de vigilance requis.

Dans l'immédiat nous vous demandons donc :

- de **respecter scrupuleusement** [la charte du numérique de l'UCA disponible ici.\(https://intranet.uca.fr/thematiques/communication/marque/identite-visuelle-de-la-marque\)](https://intranet.uca.fr/thematiques/communication/marque/identite-visuelle-de-la-marque)
- de **vous assurer que votre adresse de contact est bien renseignée et à jour dans l'ENT** pour vous permettre de gérer votre compte informatique de manière autonome, sans délai et sans intermédiaire, en cas de problème.
- de rester très vigilants, dans le cadre de la lutte contre le "*phishing*" (**hameçonnage ou récupération d'identifiants/mot de passes**) et **contre la propagation de virus**. Ces attaques arrivent en général **sous forme de mail frauduleux vous conduisant vers des sites malveillants** reprenant pour bon nombre la charte graphique de l'établissement et pouvant être formulés dans un français correct. Par ailleurs ils peuvent vous inciter aussi à ouvrir des fichiers corrompus.







*Actuellement des pourriels circulent et contiennent des fichiers au format .xlsm qu'il ne faut pas ouvrir.  
De manière général, n'ouvrez pas les pièces attachées, ni les liens internet figurant dans des mails dont  
vous n'êtes pas sûrs de l'expéditeur.*

**Nous vous invitons à transférer tout mail suspect à l'adresse [signalement.dsi@uca.fr](mailto:signalement.dsi@uca.fr)**

## **Guides pratiques**

Vous trouverez, **dans les liens suivants, des éléments pour identifier ces e-mails ou ces sites frauduleux** afin d'éviter de vous exposer ou d'exposer vos données ou outils professionnels. Vous pourrez aussi trouver de l'aide pour la gestion de votre compte informatique.

**\*NOTEZ QUE CES GUIDES PRATIQUES PEUVENT VOUS SERVIR À TITRE PRIVÉ CAR LES CAMPAGNES DE PHISHING VISENT TOUTE SORTE DE PUBLIC, PAS SEULEMENT LES ENTREPRISES.**

- Comment reconnaître un mail frauduleux : <https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=86048849>(<https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=86048849>)
- Comment reconnaître un site frauduleux de phishing : <https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=98804087>(<https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=98804087>)
- Gestion sécurisée du compte informatique : <https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=76547010>(<https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=76547010>)
- Saisir ou mettre à jour son adresse de contact : <https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=76546987>(<https://confluence.dsi.uca.fr/pages/viewpage.action?pageId=76546987>)

**L'Agence Nationale de la Sécurité de Systèmes d'Information (ANSSI) propose un guide d'hygiène informatique au format pdf sur son site web.** Pour l'obtenir, il vous suffit de taper "**Guide d'Hygiène ANSSI**" dans un moteur de recherche pour y accéder.

<https://dsi.uca.fr/actualites/8-bis-securite-numerique>(<https://dsi.uca.fr/actualites/8-bis-securite-numerique>)