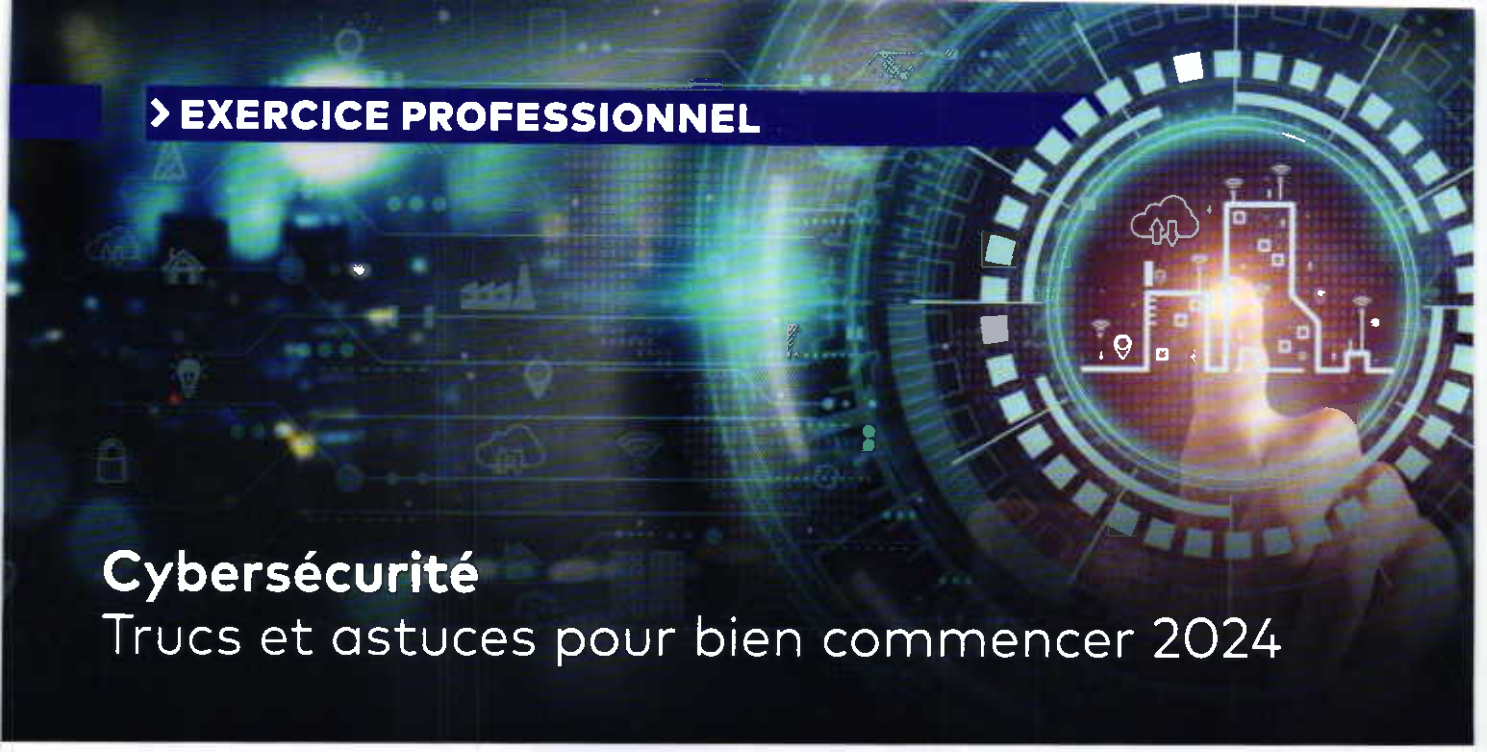

Cybersécurité
Trucs et astuces pour bien commencer 2024

PAR **HENRI MEICHE**,
CHARGÉ D'ÉTUDES,
DÉPARTEMENT DES
ÉTUDES MÉTIERS,
CONSEIL NATIONAL

L'humain est au cœur de la prévention de la cybersécurité et pour cause, 84 % des incidents sont liés à ce facteur. Comme l'écrit Platon, « ce ne sont pas les murs qui font la cité mais les hommes », et il n'y a rien de plus vrai en matière de cybersécurité. Afin de bien commencer l'année 2024, nous vous présentons quelques outils et bonnes pratiques pour muscler votre vigilance face aux tentatives de cyberattaques.

RENFORCEZ VOTRE CYBERVIGILANCE GRÂCE AUX *ADD-ONS* SUR VOTRE NAVIGATEUR !

Qu'est-ce qu'un *add-on* ?

Un *add-on*, *plug-in*, ou encore une extension, sont autant de noms s'appliquant à un composant logiciel qui étend les fonctionnalités d'un programme préexistant. Dans notre cas, les *plug-ins* pour navigateurs internet (Chrome, Firefox, Edge, etc.) permettent, par exemple, de bloquer des pubs intempestives, des traqueurs, ou encore de détecter la géolocalisation du serveur d'un site internet. Voici une liste non exhaustive de quelques *add-ons** gratuits ou freemium qui vous donneront la possibilité de surfer sur le web de façon plus sûre :

Type d'*add-on*	Noms des *add-ons*	Navigateur internet disposant de l'*add-on*		
		Chrome	Firefox	Edge
Indicateur de fiabilité des sites web	FranceVérif	Oui	Oui	Oui
	Scamdoc	Oui	Oui	Oui
	Web of Trust (WOT)	Oui	Oui	Oui
Géolocalisateur du serveur du site web	Country Flags & IP Whois	Oui	Oui	Oui
	IP Domain Country Flag	Oui	Non	Oui
	FlagFox	Non	Oui	Non
Bloqueur de traqueur web	Ghostery	Oui	Oui	Oui
	Privacy badger	Oui	Oui	Oui
	AdBlock	Oui	Oui	Oui

**Attention, les add-ons ne sont pas infaillibles, mais ils peuvent renseigner un niveau de vigilance à adopter.*

LES DIFFÉRENTS TYPES D'*ADD-ONS*

À noter que les *add-ons* proposés dans le tableau sont cumulables et particulièrement efficaces pour vous aider à lutter contre le phishing.

Pour rappel : le phishing, principale menace actuelle, est une méthode d'appât s'appuyant sur l'ingénierie sociale et consistant à escroquer en ligne en envoyant des faux e-mails, imitant ceux d'une institution ou d'une entreprise et semblant provenir d'une source fiable. Les utilisateurs sont ainsi incités à révéler des données confidentielles telles que leurs informations bancaires. De nombreux e-mails de phishing prétendent, par exemple, provenir d'une banque et invitent les destinataires à entrer leurs informations d'identification sur une fausse page web imitant le site de la banque.

L'indicateur de fiabilité des sites web
Ce type d'outil est un détecteur de sites internet d'arnaques par l'affichage d'un indice de fiabilité du site web consulté. Par exemple, si le lien d'un mail de phishing conduit vers un faux site de Bibliordre, l'outil vous signalera une fiabilité faible.

Le géolocalisateur de serveur du site web
Un *add-on* qui géolocalise le serveur du site internet consulté permet aux utilisateurs d'obtenir des détails sur l'emplacement géographique du serveur qui héberge le contenu web auquel ils accèdent.
Par exemple, si le lien d'un mail de phishing semble conduire vers le site du Conseil national et que le serveur est situé en Ukraine, vous pouvez être certain que le site est un faux.

Le bloqueur de traqueur web
Un *add-on* bloqueur de traqueur web est un outil conçu pour empêcher les entreprises et les sites web de suivre les activités en ligne, tout en réduisant la quantité de données collectées des utilisateurs.
Par exemple, lorsqu'un utilisateur accède à un site de commerce en ligne, habituellement parsemé de traqueurs pour la publicité ciblée, l'*add-on* bloque ces éléments.
Ainsi, l'utilisateur peut parcourir des produits en ligne sans craindre que ses données de navigation soient utilisées à des fins de suivi ou de profilage.

RENFORCEZ VOTRE CYBER-RÉSILIENCE GRÂCE AUX EXTENSIONS DE NOM DE FICHIER !

Qu'est-ce qu'une extension de nom de fichier ?
Ce terme se réfère à la partie d'un nom de fichier située après le point « . » dans son nom. Cette extension est souvent composée de quelques lettres ou mots et est utilisée pour indiquer le type de fichier.
Par exemple, dans le fichier « image.jpg », l'extension est « .jpg », signalant qu'il s'agit d'une image au format JPEG.

Comment faire apparaître les extensions de nom de fichier ?
Il suffit d'aller dans n'importe quel dossier sur votre bureau (Windows ou Mac) et, une fois celui-ci ouvert, de cliquer sur l'option « affichage ».
Dans le menu en haut de dossier, vers la droite, il y aura un espace intitulé « Afficher/masquer ».
Dans cet espace, cochez la case « extension de nom de fichier ».
Dorénavant, à tout endroit de votre ordinateur (notamment vos mails), vous verrez à la fin de chaque fichier s'il y a écrit : « .docx », « .pptx », « .png », etc.
Par exemple, si vous rencontrez l'extension « .exe »* dans le nom d'une pièce jointe, cela veut dire que le fichier est exécutable et va installer un logiciel sur votre machine.

**Attention, cela ne veut pas dire que tous les fichiers avec l'extension « .exe » sont des virus.*

RESTEZ VIGILANT !

Tous ces outils ne sont pas une panacée face aux cyberattaques et tout particulièrement au phishing.
En effet, comme indiqué de manière liminaire, jamais rien ne remplacera le rôle prépondérant de votre esprit critique, qui demeure votre meilleure ligne de défense sur internet.
Aucun outil technologique ne peut remplacer votre discernement et votre vigilance personnels.

Restez informé, soyez conscient des signaux d'alerte et adoptez une approche proactive pour naviguer en toute sécurité dans un monde numérique en constante évolution. En combinant ces outils avec une attitude prudente, vous renforcez significativement votre posture de sécurité en ligne.

Quelques conseils clés à retenir :
- *Vérifiez la fiabilité et la réputation des sites que vous visitez et que vous relayez et évitez certains sites dangereux (comme les sites de téléchargement ou de streaming vidéo...) ;*
- *Méfiez-vous des mails que vous recevez : ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes d'expéditeurs inconnus sans analyser le contenu du mail et regarder l'extension de nom de fichier a minima ;*
- *En cas d'expéditeurs inconnus ou de messages inhabituels, ne répondez pas, ne cliquez pas sur les liens, n'ouvrez pas les pièces attachées, ne transmettez pas vos coordonnées bancaires ;*
- *Sensibilisez vos collaborateurs pour qu'ils aient un comportement avisé et responsable ;*
- *Prudence en cas de message inhabituel mettant en doute l'origine réelle du courriel... Et en cas de soupçon, faites un contre-appel.*

POUR ALLER PLUS LOIN

Consultez le dossier thématique Cybersécurité sur www.experts-comptables.fr (site privé de l'Ordre).