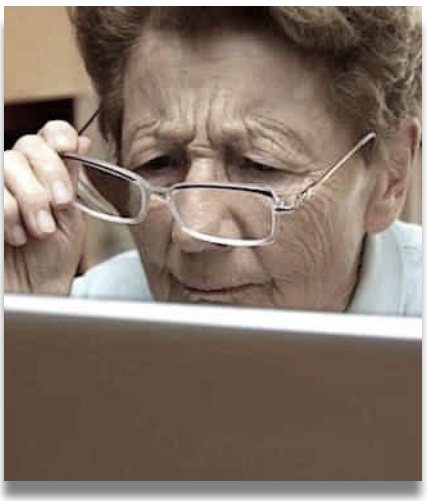
LA LETTRE DU CYBER-CONSEILLER

MAI ET JUIN 2022



Sommaire

La lettre Cyber, 15e année

Le cyber-conseiller: découvres ce que tu ignores encore…

LES ESCROQUERIES PAR INTERNET

Si vous passez du temps en ligne, vous avez probablement déjà été la cible d'une attaque de phishing. L'escroc prétend venir d'une entreprise reconnue pour que vous révéliez des informations personnelles qu'il pourra utiliser.

Le phishing est une technique souvent employée via des e-mails, des sites web, des fenêtres contextuelles et même des applications mobiles

Le conseiller L'escroquerie apparaît comme un e-mail d'une personne responsable dans l'administration ou la banque, qui vous demande des informations sensibles comme votre compte de formation, votre numéro de sécurité sociale ou d'autres informations personnelles.

Partage de fichiers De plus en plus d'imposteurs demandent l'accès à des fichiers hébergés dans des comptes Dropbox ou autres fichiers sur Cloud, et vous piègent en vous faisant cliquer sur des liens dangereux.

L'escroquerie par la séduction Celle-ci peut se dérouler entièrement en ligne, par téléphone, ou en personne lorsque le contact est établi. Ce type d'escroquerie commence toujours avec une personne qui prétend chercher l'amour. L'escroc poste une fausse annonce en ligne ou prétend être l'ami d'un ami sur les réseaux sociaux et vous contacte directement. Mais ce qui commence avec une promesse de romance ou de relation de couple se termine souvent en demande d'argent ou de cadeaux coûteux. Ils utilisent l'amour et l'acceptation pour vous piéger.

Le phishing mobile Les escrocs proposent de fausses applications mobiles qui rassemblent vos informations personnelles en arrière-plan ou vous envoient des SMS qui contiennent des liens dangereux.

Enquêtes Vous recevez une demande pour participer à une enquête pour une cause qui vous tient à cœur. Lorsque vous cliquez sur ce lien, vous pouvez être infecté par un logiciel malveillant.

Pièce jointe à un e-mail urgent Les e-mails de phishing essayent de vous piéger en vous faisant télécharger une pièce jointe dangereuse qui donne accès à votre ordinateur à des personnes mal intentionnées. Ce type d'e-mail vous demande de télécharger des pièces jointes pour confirmer la livraison d'un colis, un itinéraire de voyage ou un prix.

Escroquerie provenant d'une loterie Vous venez de gagner un prix, souvent dans un pays étranger, et vous devez payer une petite avance pour obtenir cette récompense.

Escroquerie par enquête Vous recevez une demande pour participer à une enquête pour une cause qui vous tient à cœur. Lorsque vous cliquez sur le lien, vous êtes infecté par un logiciel malveillant.

Escroquerie bancaire Vous recevez un e-mail indiquant un problème avec votre compte en banque ou votre compte PayPal qui nécessite votre attention. Vous êtes ensuite redirigé vers un faux site où vous essayez de vous connecter et les escrocs récupèrent votre nom d'utilisateur et votre mot de passe pour le véritable site.

Escroqueries de récompense Vous serez notifié du fait que vous venez tout juste de « gagner » un prix, comme de l'argent, des bijoux ou des vacances. Ces escroqueries vous demanderont d'avancer certains frais. Fuyez …

Escroqueries au financement participatif Les créateurs de ce financement participatif vous promettent un retour contre un petit investissement dans leur projet mais finissent par empocher l'argent à la place.

Escroquerie au support technique Les criminels se font passer pour des représentants de support technique et proposent de résoudre des problèmes informatiques inexistants. Ils peuvent par exemple se faire passer pour une entreprise de cybersécurité qu'ils connaissent bien. Les escrocs accèdent à distance aux équipements et aux informations sensibles des victimes ou les facturent pour des services qui n'ont jamais été nécessaires ou rendus.

Escroquerie visant les grands-parents Les criminels se font passer pour un membre de la famille, généralement un enfant ou un petit-enfant, et prétendent avoir un besoin financier immédiat.

Escroquerie d'usurpation d'identité du gouvernement Les criminels se font passer pour des fonctionnaires et menacent d'arrêter ou de poursuivre les victimes si elles n'acceptent pas de fournir des fonds ou d'autres paiements.

QUELQUES CONSEILS :

Gardez les logiciels de votre ordinateur à jour. Votre système d'exploitation, vos navigateurs web et vos applications sont constamment mis à jour pour s'adapter aux nouvelles pratiques des escrocs. Cela comprend également la mise à jour de votre abonnement.

Faites vos achats auprès de sources fiables. Réalisez quelques recherches si vous n'êtes pas sûr.

Méfiez-vous des personnes qui vous demandent plus d'informations que ce dont elles ont besoin, même si vous discutez avec une entreprise ou une banque que vous connaissez.

Posez-vous cette question simple avant de répondre à un message. Vérifiez d'abord si vous reconnaissez le nom de l'expéditeur et son adresse e-mail.

Avant de cliquer sur un lien, survolez-le pour regarder si l'adresse URL vous semble légitime.

Avant de vous connecter sur un compte en ligne, assurez-vous que l'adresse web est correcte. Les auteurs de phishing reproduisent de véritables sites web, comme des comptes de stockage en ligne, en espérant vous piéger en vous faisant saisir vos informations de connexion.

Regardez l'adresse électronique de l'expéditeur. Correspond-t-elle au contenu de l'e-mail ? Si la réponse est non, prenez vos distances.

Le lien dans l'e-mail a-t-il l'air étrange ? La plupart du temps, vous pouvez passer votre curseur sur le lien pour voir son adresse. Si elle vous paraît étrange, gardez vos distances.

N'envoyez jamais d'argent ou de cartes-cadeaux à quelqu'un que vous n'avez pas rencontré en personne.

Résistez à la pression d'agir rapidement : Les escrocs créent un sentiment d'urgence pour susciter la peur et inciter les victimes à agir immédiatement.

N'ouvrez jamais une pièce jointe d'un e-mail provenant d'une personne que vous ne connaissez pas, et méfiez-vous des pièces jointes qui vous sont transmises.

source : MacAfee

PARTAGEZ VOS FICHIERS EN TEMPS RÉEL

Si vous avez déjà tenté de joindre des fichiers de tailles importantes à vos mails, vous avez sûrement eu droit à un joli message d'erreur. Et oui la taille des pièces jointes ne peut dépasser 10 ou 25 Mo en fonction du fournisseur de votre boîte mail.
Pour pallier cette limite, il existe de nombreux sites qui proposent un service d'hébergement/envoi de fichiers lourds.
Problème éventuel : quid de la confidentialité des données ? Peut-on faire confiance à ces services ? Est-ce que les serveurs sont bien en France?

Nous vous présentons aujourd'hui un tutoriel vidéo sur le service en ligne gratuit "DirectShare". L'idée est on ne peut plus simple : proposer le partage de fichiers en temps réel ! L'intérêt? Et bien il est évident : une fois la transmission ou le partage terminé, les navigateurs fermés, vous pouvez être sûr que vos données ne se promènent pas quelque part sur le web! Pour comprendre mieux cela, je vous invite à découvrir cette vidéo.

visionner cette vidéo

GÉREZ AUTOMATIQUEMENT LES FENÊTRES WINDOWS

Disponibles gratuitement pour les utilisateurs de Windows 10 ou 11, les **PowerToys** sont des fonctionnalités supplémentaires destinées à simplifier et optimiser l'utilisation que vous faites de votre ordinateur.
Voici le lien pour télécharger le pack de PowerToys : **cliquez ici**
Dans ce tutoriel vidéo, nous allons nous intéresser au Powertoy nommé "**Fancy Zones**". Cet outil permet de gérer l'organisation des fenêtres ouvertes à l'écran. Concrètement, l'outil affiche un gabarit en transparence sur votre bureau, et se charge de redimensionner automatiquement et de maintenir les fenêtres dans les zones où vous les positionnez. Hyper pratique !

visionner cette vidéo

ORGANISEZ LES ICÔNES DE VOTRE BUREAU WINDOWS

Organiser ou déplacer des icônes Pour réorganiser les icônes par nom, type, date ou taille, cliquez-droit sur une zone vide du bureau et puis cliquez sur Réorganiser les icônes. Cliquez sur la commande qui indique comment vous souhaitez réorganiser les icônes (par Nom, par Type, et ainsi de suite). Si vous souhaitez que les icônes soient réorganisées automatiquement, cliquez sur Réorganisation automatique. Si vous souhaitez personnaliser l'organisation des icônes, cliquez sur Réorganisation automatique et décochez la case.

Supprimer des icônes

Certaines icônes sont des raccourcis vers des programmes sur votre ordinateur. Les icônes de raccourci disposent généralement d'une flèche dans le coin inférieur gauche. Si vous ne voulez pas un raccourci sur votre bureau, cliquez sur l'icône et puis faites-la glisser vers la corbeille. Cette action supprime uniquement le raccourci, pas le programme vers lequel il est dirigé. Vous pouvez aussi effectuer un clic droit sur l'icône et puis cliquer sur Supprimer pour supprimer un raccourci de votre bureau.

Certaines icônes comme Emplacements réseaux, Corbeille, et Poste de travail ne peuvent pas être supprimées.

Modifier l'image des icônes.

Les images de certaines icônes peuvent être modifiées. Ce paramètre n'est pas disponible pour toutes les icônes. Pour changer l'image de l'icône :

1. Cliquez avec le bouton droit sur l'icône, puis cliquez sur Propriétés.
2. Cliquez sur l'onglet raccourci (s'il est disponible), puis sur Modifier l'icône.
3. Cliquez sur l'icône que vous souhaitez utiliser dans la liste, cliquez sur OK, puis cliquez sur OK.

S'il n'y a pas d'icônes disponibles dans la liste, le fabricant n'a peut-être pas fourni d'icônes supplémentaires. Pour trouver d'autres icônes, suivez la même procédure sur une autre icône, recherchez son fichier source (généralement un fichier .ico), puis retournez à l'icône d'origine à modifier. Suivez la même procédure, mais lorsque vous cliquez sur le bouton Modifier l'icône, naviguez jusqu'à l'emplacement du fichier source de l'icône différent.

REMARQUE : Des outils tiers sont disponibles pour vous permettre de modifier les icônes ou de créer des fichiers .ico à partir d'images.

source : Microsoft

ANDROID : QUELQUES ASTUCES

GPS toujours actif avec une consommation de batterie minimale

Le système de positionnement global ou GPS est l'une des rares choses qui ont parcouru un long chemin. Du suivi de la localisation au guidage d'itinéraire, la navigation actuelle dépend beaucoup du GPS. Mais avec la réduction de la taille des batteries et l'extension croissante des systèmes de navigation, il est presque impossible de toujours garder le GPS allumé et d'économiser la batterie en même temps.

Cependant, il existe une solution rapide qui vous permet simplement de basculer en mode économie de batterie tout en maintenant le GPS activé.

Pour l'activer, allez dans les paramètres d'emplacement et sélectionnez le mode d' économie de batterie. Lorsque vous passez en mode économie de batterie, l'appareil arrête de rechercher activement des satellites pour se localiser. Au lieu de cela, il bascule vers la triangulation de tours cellulaires où il se rapproche de sa position en fonction des tours cellulaires les entourant.

Ce n'est pas aussi précis que le GPS par satellite, mais consomme beaucoup moins d'énergie, ce qui maintient votre batterie sans pression.

Déverrouillage automatique

Vous devez vous demander pourquoi quiconque voudrait déverrouiller les appareils automatiquement et en quoi cela affecterait la sécurité. Ne crains pas! Android possède une fonctionnalité intégrée intelligente, qui permet à l'appareil de se déverrouiller automatiquement lorsqu'il identifie un emplacement familier. Cela peut être votre maison, votre bureau ou tout autre endroit de votre choix. Une fois que l'appareil a quitté cet endroit, il repasse automatiquement en mode de déverrouillage manuel. Cela peut également fonctionner avec un périphérique Bluetooth. Par exemple, si vous écoutez de la musique et souhaitez garder votre appareil déverrouillé, ajoutez simplement votre haut-parleur Bluetooth en tant qu'appareil de confiance et votre téléphone ne se verrouillera pas tant que vous ne serez pas connecté à cet appareil bluetooth. Pour l'activer, accédez à l'onglet Verrouiller l'écran et le mot de passe, choisissez Déverrouiller avec un périphérique Bluetooth, puis sélectionnez le périphérique dans l'écran suivant.

Bloquez la publicité

Vous en avez assez d'être traqué.e par les publicités ? Alors, bloquez-les !
En effet, lorsque vous naviguez sur les sites web, changez votre DSN privé par un service de blocage de publicité. Pour cela, rendez-vous dans :

Paramètres > Connexion et partage > DNS privé > ;

Changez-le pour **"dns.adguard.com"** ;
Validez et enregistrez.

Grâce à cette astuce, plus aucune publicité ne gênera votre navigation. Pour info, Adguarda est un système performant qui assure votre confidentialité en ligne.

Pour les plus aguerris qui ne souhaitent pas que Google récupère leurs données comme leur position géographique ou les sites qu'ils visitent, optez pour le process suivant qui consiste à supprimer une option intrusive :

Paramètres > Annonces > Réinitialiser l'identifiant publicitaire > OK ;

Vous supprimez votre profil qui est ciblé ;

Puis vous en créez un nouveau et vous validez ;

Activez « personnalisation des annonces » puis validez.

Enfin, si vous ne voulez pas que Google enregistre tous vos déplacements, scrollez jusqu'en bas des paramètres et dans Localisation > Historique des positions Google > Compte principal > et là vous décochez Historique des positions et Suspendre en bas à droite.

☆☆☆