CiNM
Club Informatique et Numérique Menneçois

Newsletter

Avril 2024 | 74

Si l'intelligence artificielle ouvre de beaux horizons aux escrocs numériques, elle pourrait aussi nous aider à nous en prémunir. En attendant, certains antivirus proposent déjà de nous protéger de pratiques frauduleuses nouvelles. Cette Newsletter fait le point sur le sujet.

Denis GELIN

Sécurité Internet - L'IA rebat les cartes *(1/2)*

Et si cette année était celle de la numérisation de toutes les démarches administratives ? Tel était, en tout cas, le souhait du gouvernement lorsqu'il a lancé, en 2017, le plan Full Démat'. Ce dernier prévoyait la dématérialisation de 250 procédures administratives parmi les plus courantes d'ici à la fin de 2023. Mais l'objectif n'est qu'en partie atteint. Une vingtaine d'entre elles restent à numériser. Quant aux 230 autres formalités officiellement réalisables sur Internet, leur degré de numérisation varie.

C'était il y a moins d'un an. Jennifer, une Américaine de l'Arizona, recevait un appel téléphonique inquiétant. Au bout du fil, sa fille de 15 ans, en larmes, lui expliquait entre deux sanglots avoir été enlevée par des individus. Dans la foulée, un homme affirmant séquestrer l'adolescente menaçait de lui faire du mal si la mère ne lui versait pas rapidement la somme de 50 000 dollars.

Heureusement, une amie qui lui tenait compagnie a eu l'idée d'appeler immédiatement le père de la jeune fille, qui lui a indiqué que l'adolescente se trouvait à son côté, saine et sauve. Jennifer a coupé court à la conversation sans verser d'argent. Mais, plus tard, elle a assuré n'avoir pas douté une seconde, en entendant l'audio, que sa fille lui parlait au téléphone. L'enquête a révélé que celui-ci avait été créé par une intelligence artificielle.

À la même période, d'autres Américains vivaient des expériences similaires. Un couple était destinataire d'un message vocal de son fils dans lequel celui-ci expliquait avoir été arrêté par la police avant qu'un « avocat » ne demande de l'argent pour le paiement de la caution. La secrétaire d'une entreprise, elle, recevait de son patron la consigne d'effectuer sans attendre un virement vers un fournisseur. Tous ces messages se sont finalement révélés être des faux et avaient pour point commun d'avoir été créés grâce une intelligence artificielle dans le seul but d'extorquer de l'argent.

Les escroqueries visant le grand public semblent pour l'heure se limiter à de courts messages vocaux en anglais. Mais nul doute qu'au fur et à mesure que les IA se perfectionneront la voix et le visage de tout un chacun pourront être imités, voire que l'avatar ainsi obtenu sera capable de tenir avec la victime une véritable conversation…

Des possibilités infinies…

L'apport de l'IA en matière de menaces informatiques ne s'arrête pas là. Grâce à cette nouvelle technologie, les escrocs seront bientôt en mesure de concevoir des messages d'hameçonnage (ou phishing) sans la moindre faute d'orthographe ou de syntaxe, imitant à la perfection les originaux et adaptés aux pays vers lesquels ils sont envoyés.

L'IA pourrait aussi aider les pirates à identifier les mots de passe de leurs victimes, à coder de nouveaux logiciels malveillants (ou malwares), à créer de faux sites marchands, ou encore à analyser des systèmes informatiques pour y repérer des failles. Elle pourrait même faciliter la tâche des « brouteurs » (ces escrocs spécialistes des arnaques aux sentiments ou au faux héritage) en aidant à engendrer des vidéos truquées ou en menant à leur place des conversations très réalistes avec les victimes en vue de leur soutirer de l'argent. De telles arnaques nécessitent pour le moment un minimum de connaissances en informatique et de matériel mais, grâce aux avancées de la technologie, tout va devenir plus simple.

L'état de la menace

- l'hameçonnage (ou phishing) constitue toujours le risque n° 1. Il passe de plus en plus par les SMS (smishing),
- renouvellement de carte Vitale, mise à jour de CPF, colis en attente… les cybercriminels s'appuient plus que jamais sur l'actualité pour voler les infos personnelles ou les données bancaires de leurs victimes,
- arnaques au faux conseiller bancaire et fraudes au virement se sont multipliées ces dernières années.

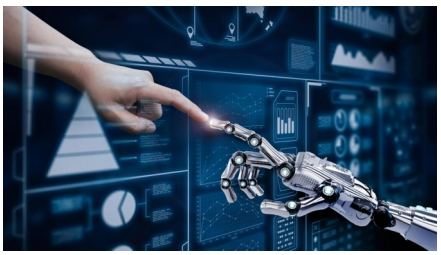
Aujourd'hui, pour créer un deepfake (une vidéo usurpant le visage et la voix d'un individu), il faut nourrir l'IA de dizaines de photos, de vidéos et de sons de cette personne. Bientôt, une poignée de clichés et quelques secondes de voix suffiront.

Surtout, ces outils seront facilement accessibles au plus grand nombre, à tel point que chacun pourra devenir un pirate en puissance. Les intelligences artifi-

Sécurité Internet - L'IA rebat les cartes *(2/2)*

cielles telle que ChatGPT ont-elles été programmées de manière à refuser de créer de nouvelles menaces ? Peu importe. On trouve sur le darknet des IA moins regardantes ! La plus connue d'entre elles, FraudGPT, offre d'ores et déjà la possibilité à n'importe qui de créer des malwares, de produire des messages de phishing ou encore de rechercher des vulnérabilités dans les logiciels. Ce genre d'outils va, à coup sûr, se multiplier et se perfectionner.

L'intelligence artificielle générative n'aura de limite que celle de l'imagination des pirates, prévient un expert. Grâce à elle, les menaces de demain seront davantage sophistiquées, poussées et réalistes, et donc plus difficiles à déceler. Elle permettra aussi aux pirates de lancer facilement des attaques de bien plus grande ampleur qu'aujourd'hui. Pour autant, tente-t-il de relativiser, elles s'appuieront sur les mêmes ressorts que celles actuelles. Les escrocs auront beau générer de fausses vidéos ou rédiger des messages de phishing plus vrais que nature, ils continueront à contacter leurs victimes par e-mail ou par téléphone, à chercher à récolter leurs données personnelles ou à essayer de leur extorquer de l'argent.



Gare aux attaques totalement innovantes

Pour l'heure, l'IA n'a pas changé radicalement la donne en matière de cybersécurité, confirme un autre expert. Les menaces qu'elle fait naître reposent sur les mêmes fondements que celles d'avant. Il faut toutefois rester vigilant car rien ne dit qu'un jour une IA ne créera pas une attaque informatique complètement innovante à laquelle personne n'avait pensé jusque-là et qui réussira à déjouer les mécanismes de protection, de détection et de réponse. On a déjà vu cela dans d'autres domaines.

Des éditeurs dans les starting-blocks

L'intelligence artificielle interviendra au premier plan dans la création des futures menaces mais elle va aussi nous aider à mieux nous en prémunir. D'ailleurs, tous les spécialistes de sécurité internet l'ont déjà intégrée à leurs outils de détection. L'IA est omniprésente dans nos solutions ainsi que dans les objets que nous protégeons explique un professionnel expert en cyberdéfense. Elle nous est très utile, par exemple, pour mieux repérer les logiciels ayant des comportements suspects, ou encore distinguer les échanges de données anormaux, signes possibles d'une tentative d'arnaque. Certains acteurs ont ainsi déployé des logiciels spécifiquement fondés sur l'IA, à l'image de McAfee et de sa fonctionnalité Scam Protection, censée détecter les menaces. C'est le cas aussi de Bitdefender, qui met gratuitement à la disposition de tous une solution d'aide au repérage des arnaques en ligne baptisée Scamio. Également créé avec l'intelligence artificielle, c'est un robot conversationnel (chatbot) capable d'évaluer le risque que représente tel ou tel message, comme le ferait n'importe quel spécialiste en cybersécurité. Les réponses ont beau être uniquement en anglais, le résultat est plutôt convaincant. Pour autant, ce genre d'initiative doit être pris avec précaution, car la forte présence de l'IA dans l'actualité et la compétition acharnée sur ce marché ont tendance à pousser les éditeurs de solutions de sécurité à mettre en avant cette technologie dans leur communication, quitte à enjoliver ce dont elle est capable. Or, si cet outil peut bel et bien aider à augmenter les performances de détection des antivirus grâce à sa capacité à multiplier les contrôles et à analyser plus finement les comportements suspects, il ne faut pas compter dessus pour éradiquer toutes les menaces existantes. Pirates et éditeurs vont continuer longtemps à jouer au chat et à la souris. Et, à ce jeu-là, les escrocs auront toujours une longueur d'avance.

PRATIQUE

REDOUBLER DE VIGILANCE

Des arnaques très bien conçues, plus innovantes, mieux ciblées... Face à une « professionnalisation » de la menace, les internautes doivent faire preuve d'encore plus de prudence. Plus que jamais, il faut avoir à l'esprit que ce qui a l'air vrai ne l'est pas forcément. Pour autant, les arnaques s'appuient sur les mêmes ressorts qu'hier. Il importe donc de conserver les bons réflexes.

REJETER LES MESSAGES DOUTEUX

Ils ont beau être plus sophistiqués et mieux rédigés qu'avant, les e-mails provenant d'inconnus doivent toujours être pris avec précaution, N'ouvrez pas les pièces jointes, ne cliquez sur aucun lien et n'y répondez pas, surtout quand on vous met la pression pour le faire rapidement. Selon les cas, vous risqueriez de voir votre ordinateur infecté, d'être renvoyé vers un Site malveillant ou de vous engager dans une conversation qui n'aura d'autre but que de vous soutirer de l'argent. Il en est de même pour les SMS et les appels téléphoniques.

INSTALLER UNE SUITE DE SÉCURITÉ INTERNET

Même si elles ne sont pas infaillibles, elles permettent de stopper une bonne partie des menaces Une suite gratuite peut très bien faire l'affaire.

NE PAS BLOQUER LES MISES À JOUR

Les mises à jour automatiques réalisées par les systèmes d'exploitation, les navigateurs et les autres programmes servent à réparer les failles dont profitent les pirates. Elles sont donc essentielles à la sécurité.

RENFORCER SES MOTS DE PASSE

Optez pour des mots de passe différents et sécurisés pour chaque service. Sans oublier votre messagerie, et acceptez la double authentification lorsqu'elle est proposée (vérification via le téléphone, notamment). Le gestionnaire de mots de passe offert par la plupart des suites payantes être une bonne solution.

SE MEFIER DES TROP BELLES AFFAIRES

Une application donnant un accès illimité à des jeux, un site pour transformer ses documents en PDF... Gardez-vous des logiciels et utilitaires proposés gratuitement ! Ils peuvent receler des codes malveillants qui, une fois sur votre ordinateur, afficheront de la publicité intempestive, voleront vos données ou détecteront vos mots de passe en analysant ce que vous tapez sur le clavier. En cas de doute, soumettez le fichier, avant de l'exécuter, à un service d'analyse en ligne (Jotti.org ou VirusTotal.com. par exemple). Si vous n'êtes pas sûr, ne le lancez pas.

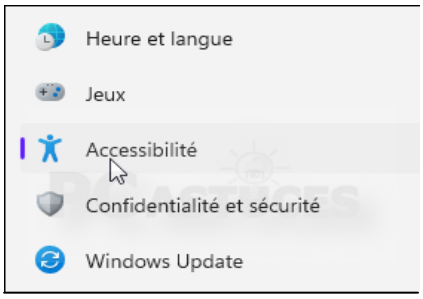
Windows 11 - Personnaliser la taille et la couleur du curseur de texte

Avec Windows 11, vous pouvez personnaliser la taille et la couleur du curseur de texte afin de le rendre plus visible.

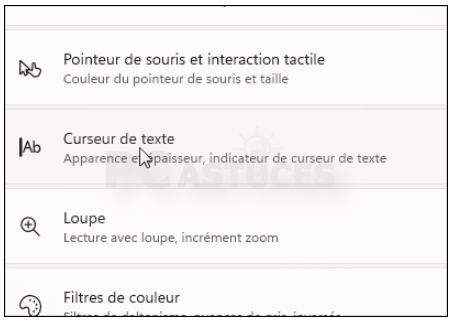
1. Cliquez sur le bouton **Démarrer**.

2. Cliquez sur **Paramètres**.

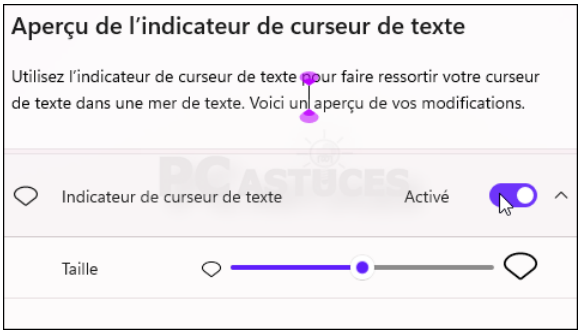
3. Dans la colonne de gauche, cliquez sur **Accessibilité**.



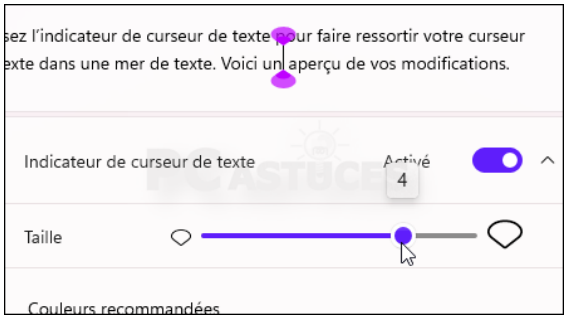
4. Dans la colonne de gauche, cliquez sur **Curseur de texte**.



5. Activez l'option **Indicateur de curseur de texte**.

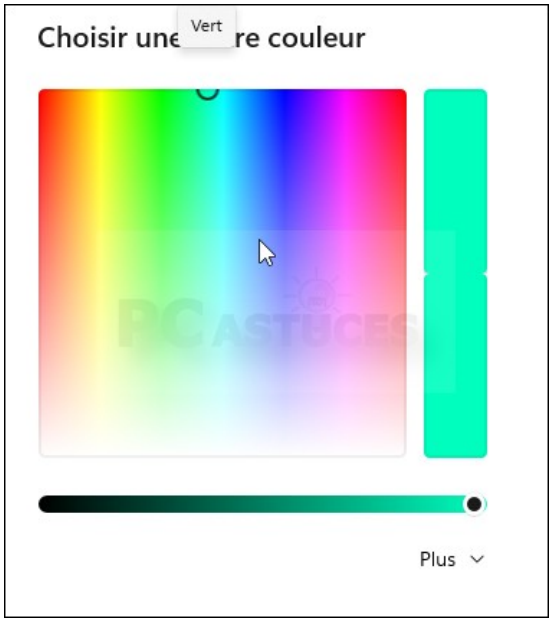


6. Modifiez la taille du curseur avec la barre horizontale.



7. Choisissez une couleur dans la liste proposée.

8. Pour sélectionner une couleur dans une palette complète, cliquez sur **Choisir une autre couleur** et validez.



9. Désormais, le curseur qui apparaît là où vous pouvez saisir du texte dans n'importe quel logiciel, est nettement plus visible.

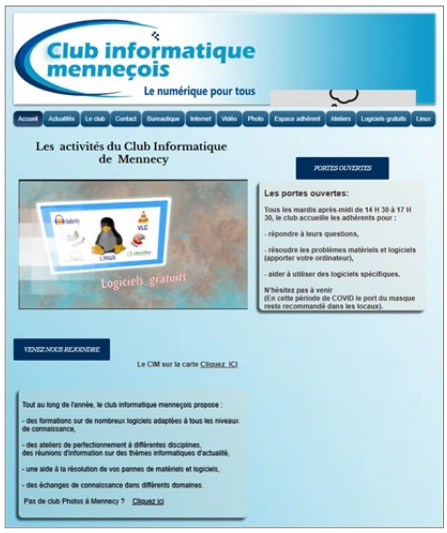
Un nouveau site Internet pour le club

Après une année de travail intensif, l'équipe de Monique WEBER, Jacques GOURDON et Thierry DELAPORTE ont mis en ligne le nouveau site Internet du club en janvier dernier.

Pourquoi un nouveau site ?

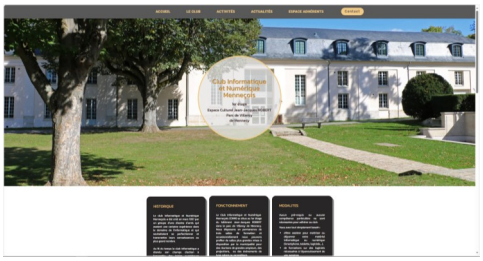
Un site Internet est souvent le premier contact pour un futur adhérent. Il constitue donc la vitrine du club et doit être représentatif de son activité, de sa compétence et de son dynamisme.

Or, l'ancien site avait vieilli après des mises à jours successives sans réel fil conducteur. Le visiteur pouvait s'y perdre facilement sans trouver vraiment ce qu'il recherchait.

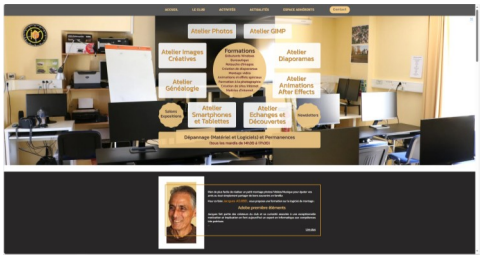


Le nouveau site offre une meilleure visibilité avec davantage de convivialité, de modernité et d'interactivité.

La page « Le club » présente le Conseil d'Administration, l'historique du club et son fonctionnement ainsi que le montant de la cotisation.

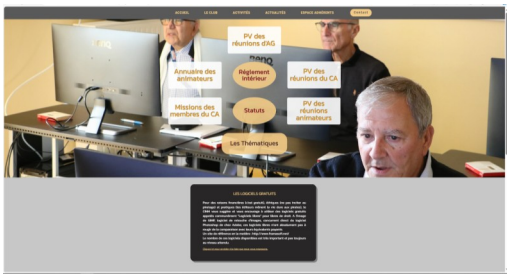


En cliquant sur l'onglet « Activités », toutes les prestations du club sont présentées de façon synthétique puis plus détaillée pour chacune d'elles.



La page « Actualité » présente le calendrier des activités et les informations du moment.

Enfin, comme auparavant, un onglet « espace adhérents » réserve la partie privée des informations aux seuls adhérents. Cette page n'est accessible qu'avec un mot de passe qui est changé tous les ans.



On y retrouve entre autres :

- les statuts du club et son règlement intérieur,
- les procès-verbaux des réunions institutionnelles.
- le descriptif des thématiques,
- la liste des logiciels gratuits préconisés par le club,
- les coordonnées des animateurs.

Se connecter au site du club.

La page d'accueil

La page d'accueil propose un diaporama présentant l'accès au club, nos locaux et nos missions.

5ème Salon de l'Image Numérique

Notre Salon s'est déroulé les 23 et 24 mars derniers. Il a accueilli près de 350 visiteurs.

Que tous ceux qui ont contribué à sa réussite en soient sincèrement remerciés.

Un compte rendu complet en sera fait dans la prochaine Newsletter.

Les colonnes de la Newsletter vous sont ouvertes : faites-nous parvenir les sujets que vous souhaitez voir publiés.