

Le numérique avec des mots [azerty]

n°1

**SÉCURITÉ
NUMÉRIQUE**

Se protéger en ligne

Pourquoi et comment

Hackers en formation

À l'IUT informatique de Maubeuge,
l'attaque est la meilleure défense

e-Enfance

Comment Justine Atlan accompagne
enfants et adolescents en ligne

Futur de la sécurité

Et si les mots de passe
disparaissaient ?

Google™

Chère lectrice, cher lecteur,

Que ce soit sur ordinateur ou téléphone, le clavier AZERTY est notre interface avec la machine et le monde numérique. Grâce à lui, nous pouvons transformer nos idées en mots et les communiquer. Apparu il y a plus d'un siècle, il s'est imposé de lui-même au fil des années.

Sur papier, l'Azerty que vous tenez entre les mains a la même ambition : un objet concret, une passerelle entre le numérique et le physique, deux mondes qui ne font finalement qu'un. Tout simplement parce que la technologie impacte plus que jamais notre vie, que ce soit au quotidien ou à une échelle plus globale. Avec Azerty, nous voulons vous accompagner dans cette plongée au cœur des multiples enjeux du numérique, et vous raconter ses défis les plus audacieux et ses plus belles histoires.

Pour ce premier numéro, nous avons souhaité mettre en lumière la question de la sécurité. Alors que l'identité se digitalise et que les objets deviennent connectés, il de-

vient impératif de comprendre pourquoi et comment se protéger en ligne. D'autant plus que cette notion n'est pas qu'individuelle, elle est aussi collective : les entreprises, les institutions et les territoires se retrouvent tout autant concernés.

À tous les niveaux, l'humain intervient pour faire de la technologie un allié du quotidien, et contrer les sources de nuisance. Mélanie aide les Rennais à naviguer sereinement. Dans ses vidéos YouTube, Michaël enquête sur les fraudes. Eduardo cherche les failles de sécurité pour les éradiquer. Stephan et Mark réfléchissent aux menaces potentielles à venir. Justine forme les enfants à se protéger. Certains travaillent pour Google, d'autres sont des personnalités extérieures à qui nous avons choisi de donner librement la parole. Tous ont leur histoire. À vous de la découvrir.

Bonne lecture, et bien sûr, bonne navigation
Votre équipe Google

Édito

Sommaire

4

J'AI UNE QUESTION

Les experts répondent



6

FUTUR DE LA SÉCURITÉ

Et si les mots de passe disparaissaient ?



9

OK GOOGLE

J'ai encore une question

10

HACKERS EN FORMATION

À Maubeuge, on attaque les systèmes informatiques pour mieux les sécuriser

12

EN PREMIÈRE LIGNE

Google développe des technologies de pointe pour protéger les utilisateurs



15

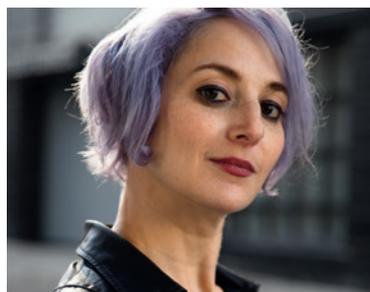
FACTEUR HUMAIN

Comment la psychologie cognitive peut enrayer les cyberattaques

16

LE COMBAT D'EVA

Sa mission : venir en aide aux femmes victimes d'espionnage numérique



18

LE JOUR OÙ

Quatre Français racontent comment ils ont compris l'importance de la sécurité numérique

20

CYBER JOURNÉE À RENNES

La cybersécurité à la portée de tous



24

NAVIGUER, CA S'APPREND

L'association de Justine Atlan accompagne les jeunes dans leur navigation



J'ai une question

Que se passe-t-il avec nos données sur Internet ?
Où apparaissent-elles, qui y a accès, et comment mieux les protéger ?
Des experts vous répondent.

Quelles traces laisse-t-on derrière soi lors d'un passage en ligne ?

Jérôme Notin,

Directeur général de Cybermalveillance.gouv.fr

L'internaute fournit, parfois sans en avoir conscience ou sans le vouloir, de nombreuses informations le concernant, sur son identité ou ses moyens de paiement, sur des sites marchands par exemple. Un site Internet peut en effet mettre à profit une simple visite pour récupérer des données techniques sur l'ordinateur qui se connecte, comme son adresse IP, le navigateur Internet utilisé ou sa géolocalisation.

Comment des personnes mal intentionnées peuvent-elles accéder à mes données ?

Jérôme Notin,

Directeur général de Cybermalveillance.gouv.fr

Des individus malveillants peuvent accéder à vos données de différentes manières : parce que vous utilisez un mot de passe trop simple qu'ils ont pu deviner ou « forcer » ; parce que vous le leur avez donné sans en avoir conscience, suite à la réception d'un message malveillant qui n'aurait pas été identifié en tant que tel (hameçonnage) ; parce que vous réutilisez un même mot de passe sur plusieurs sites, dont l'un a été piraté ; parce que vous avez communiqué votre mot de passe à un tiers qui n'a pas su le garder en sécurité ; parce que votre mot de passe est laissé à la vue d'autres personnes ; parce que votre équipement a été piégé par un virus qui envoie vos mots de passe à un cybercriminel...

Quelle est la conduite à adopter lorsqu'on reçoit un mail suspect ?

Vincent Courson,

Responsable communication, équipe Trust & Safety* de Google

Les scammers et autres pirates informatiques redoublent d'inventivité pour tenter de nous soutirer nos informations personnelles en utilisant des techniques dites de "phishing" (hameçonnage). Ainsi, il est primordial de s'entraîner à reconnaître les signes qui indiquent que l'on se retrouve confronté à une tentative de phishing. Je recommande à tous de faire le test sur phishingquiz.withgoogle.com pour être au fait des vérifications à effectuer. Si vous confirmez que vous venez bien de recevoir un message de phishing, le plus important est de ne jamais cliquer sur un lien ou une image présents dans le message, de ne pas répondre au mail et de le signaler immédiatement comme spam dans l'interface du produit que vous utilisez.

À quel point un mot de passe doit-il être compliqué ?

Régis Le Guennec,

Consultant et coach en cybersécurité

123456, c'est trop simple. Dans l'idéal, il faut un mot de passe de 10 à 12 caractères, comprenant majuscule, minuscule, chiffre et caractère spécial. Les pirates enfoncent les mots de passe en essayant, comme des serruriers, de passer toutes les clefs possibles jusqu'à tomber sur la bonne. Un ordinateur normal calcule un million de mots de passe à la seconde. Il faut faire en sorte de décourager l'attaquant pour qu'au bout d'un certain nombre d'heures, de jours ou de semaines, il passe au voisin, un peu comme les taupes. Bien sûr, il en faut un par plateforme. Je donne souvent cette image : si vous regardez votre trousseau de clefs, celle de la porte du garage n'est pas identique à celle de la maison, ni à celle de la voiture. En plus, la clef de ma penderie est bien moins forgée que celle de mon portail d'entrée.

Un smartphone est-il moins vulnérable aux attaques qu'un ordinateur ?

Vincent Courson,

Responsable communication, équipe Trust & Safety* de Google

Non ! On peut remarquer une certaine tendance à associer les mots « virus » ou « malware » aux ordinateurs plutôt qu'aux smartphones, et ce pour des raisons historiques. Mais, par exemple, Google Play Protect, le système de protection contre les malwares embarqués dans Android, scanne et vérifie plus de 50 milliards d'applications par jour. Ainsi, les menaces ne sont pas moins importantes sur smartphone, elles sont différentes. Pour profiter des protections adéquates, je conseille vivement de ne télécharger que depuis les magasins d'applications officiels... Une autre particularité du smartphone est qu'il peut se faire voler plus facilement qu'un ordinateur. Il est donc essentiel de toujours verrouiller son accès, et de savoir comment le localiser ou effacer les données qu'il contient à distance.

Est-ce qu'un réseau WiFi est sûr ?

Jérôme Notin,

Directeur général de Cybermalveillance.gouv.fr

La sécurité à 100 % n'existe pas et n'existera jamais. S'il s'agit d'un réseau privé, comme celui que l'on possède généralement au travers de sa box Internet à son domicile, il est bien protégé si l'on respecte les recommandations des fournisseurs d'accès (FAI) et les règles pour gérer ses mots de passe. En revanche, on recommande de ne pas se connecter aux réseaux WiFi publics pour accéder à des informations sensibles comme sa messagerie, ses comptes de réseaux sociaux ou son compte bancaire. Privilégiez toujours votre connexion 3G ou 4G, et désactivez votre connexion WiFi lorsque vous ne l'utilisez pas.

Qui pourrait s'intéresser à mes données ? Et pourquoi ?

Régis Le Guennec,

Consultant et coach en cybersécurité

Il y a trois types d'attaques. Un, des attaques de masse qui, comme le chalutier, vont ramasser tout ce qu'il y a au milieu de l'océan sans distinguer les plantes des cailloux. On récupère vos données personnelles pour ensuite aller discuter avec vos amis, leur expliquer que vous êtes en voyage à l'étranger et leur demander de vous faire un virement, etc. Deux, les attaques les plus courantes, réalisées par des amateurs qui ne s'intéressent qu'à l'argent qu'ils peuvent gagner en revendant vos données personnelles. Une identité complète, composée de plusieurs colonnes, peut valoir 50 dollars la ligne au marché noir. Une adresse électronique, c'est quelques centimes. Trois, les attaques menées par des proches : ex-mari, ex-femme, ex-voisin, ancien collaborateur, ancien stagiaire... La motivation : se venger ou vous faire chanter.



“Idéalement,
nous aimerions
abolir les mots
de passe”



Mark Risher est expert en cybersécurité chez Google, **Stephan Micklitz** dirige le développement global de l'équipe Sécurité et protection des données. De quoi avoir quelques idées sur la sécurité en ligne de demain, entre disparition des mots de passe et émergence des nouveaux objets connectés.

La sécurité en ligne est un combat de tous les instants. Est-ce qu'il vous arrive personnellement, vous qui êtes pourtant experts, de baisser la garde ?

- **Mark Risher** : Je n'ai pas vraiment d'exemple concret à vous donner, mais ça a bien dû m'arriver. Comme tout le monde, je fais des erreurs lorsque je navigue sur Internet. Par exemple, il n'y a pas si longtemps, j'ai saisi mon mot de passe Google sur un autre site.
- **Stephan Micklitz** : C'est un réflexe humain. Une fois que nous, utilisateurs, sommes parvenus à nous souvenir d'un mot de passe, il nous arrive de le saisir au mauvais endroit sans le faire exprès.

- **Mark Risher** : Idéalement, nous aimerions abolir l'emploi des mots de passe pour les remplacer par quelque chose de plus efficace, mais malheureusement ça n'est pas si simple.

Que leur reprochez-vous ?

- **Mark Risher** : Les mots de passe sont pleins d'inconvénients: ils sont faciles à pirater, il est très difficile de s'en souvenir et ils sont très délicats à gérer. On a tendance à penser qu'il suffit qu'un mot de passe soit long et complexe, ce qui est bien mais ne fait pas tout. En effet, il est difficile pour notre cerveau de retenir plusieurs mots de passe complexes. Ainsi, ce qui arrive fréquemment lorsqu'on en a trouvé un, c'est que l'on a tendance à l'utiliser pour sécuriser plusieurs comptes différents et c'est ainsi que l'on se met en danger.

- **Stephan Micklitz** : C'est aussi pourquoi mieux vaut ne pas toujours se déconnecter et se reconnecter. Sur le long terme, cela conduit à ne plus vraiment se souvenir sur quel site on est déjà inscrit, et cela facilite la tâche des hackers. Nous conseillons ainsi à nos utilisateurs de rester connectés autant que possible.

Pourtant, le site d'une banque, par exemple, déconnecte l'utilisateur au bout de quelques minutes d'inactivité.

- **Stephan Micklitz** : Malheureusement, de nombreuses entreprises suivent des règles dépassées. La recommandation de se déconnecter à chaque fois nous vient d'une époque où la plupart des gens se connectaient depuis des cybercafés ou partageaient leur ordinateur. Notre étude montre que plus on tape son mot de passe pour se connecter à son compte, plus on a de chances d'être victime d'un piratage.

- **Mark Risher** : Dans le pire des cas, les utilisateurs se résignent: « Je ne peux pas être complètement protégé, donc pourquoi changer mes habitudes en ligne ? » C'est comme laisser la porte de sa maison grande ouverte parce que, de toute façon, on sait qu'il y a un cambrioleur dans les parages.



Stephan Micklitz est l'un des ingénieurs spécialisés du GSEC, le centre dédié à la Sécurité de Google basé à Munich.

Comment Google pourrait-il garantir la sécurité de ses utilisateurs si les mots de passe étaient abolis ?

- **Mark Risher** : De nos jours, de nombreuses mesures de sécurité sont appliquées en arrière-plan. Nous nous employons à garantir la sécurité de votre compte Google, même si un hacker trouve votre mot de passe et votre numéro de téléphone. Par exemple, nous vérifions avec quel appareil et depuis quel pays votre compte se connecte. Ou, si quelqu'un essaie de se connecter avec votre compte et saisit un mauvais mot de passe plusieurs fois en peu de temps, cela déclenche un signal d'alerte dans notre système de sécurité.

D'après vous, où se trouvent les plus grands dangers en ligne ?

- **Mark Risher** : Le premier problème, ce sont ces listes qui traînent sur Internet contenant noms d'utilisateurs et mots de passe. Une de nos équipes a fouillé pendant six semaines les pages accessibles publiquement et elle a trouvé 3,5 milliards de combinaisons nom d'utilisateur/mot de passe ! Si ces données ne proviennent pas de comptes Google, comme beaucoup d'utilisateurs utilisent le même mot de passe plusieurs fois, ces listes

Au cœur de la sécurité

Basé à Munich et inauguré en mai dernier, le GSEC (Google Safety Engineering Center) est l'épicentre de Google pour la sécurité en ligne. De nombreux produits liés à la sécurité en ligne sont ainsi créés et testés auprès des utilisateurs européens avant d'être lancés mondialement. Le choix de l'Allemagne n'est pas anodin, comme l'a expliqué Sundar Pichai, PDG de Google : « Ce n'est pas un hasard si nous construisons notre centre de sécurité au cœur de l'Europe, dans un pays qui reflète de bien des manières comment les Européens pensent en matière de sécurité en ligne, protection et confidentialité. » D'autant plus que le GSEC est le fruit d'une riche tradition bavaroise : depuis plus de dix ans, le bureau munichois œuvre sur ces problématiques, avec notamment la mise au point du compte Google, lancé en 2011. Pour poursuivre sur cette lancée, le nombre d'ingénieurs spécialisés recrutés au sein du GSEC devrait doubler d'ici la fin de l'année.

deviennent également un problème pour nous. Le deuxième plus gros problème, d'après les statistiques, ce sont les spams, qui en plus d'être intrusifs peuvent introduire un risque en termes de sécurité. Un mail sur deux relève du spam. Dans Gmail, nous parvenons à bloquer 99,9 % de ces spams, ce qui signifie que la plupart des utilisateurs n'en reçoivent presque plus. Malgré ce progrès, le "spear phishing" (hameçonnage ciblé) reste un danger dont il faut se méfier particulièrement.

- **Stephan Micklitz** : C'est un énorme problème: le pirate envoie un message tellement personnalisé que la personne ne se rend pas compte qu'elle est victime d'une arnaque.
- **Mark Risher** : Le spear phishing est d'autant plus vicieux que sa mise en œuvre est moins complexe qu'elle en a l'air. Personnaliser un spam ne prend généralement que quelques minutes. Pour ce faire, le hacker se sert des informations publiques que la personne a partagées sur Internet.

À quel type de menaces devons-nous nous attendre à l'avenir ?

- **Mark Risher** : La mise en réseau des appareils et des services est un immense challenge pour nous. L'époque où seuls les ordinateurs portables et les smartphones étaient connectés est révolue; aujourd'hui, on a aussi les télévisions, les montres intelligentes ou encore les enceintes connectées. Et chacun de ces appareils accepte des applications différentes, et donc offre différents points d'attaque pour les hackers. Étant donné que ces appareils sont reliés entre eux, les pirates peuvent essayer d'accéder à l'un en passant par un autre. Pour nous, la question qui se pose, c'est: « Comment pouvons-nous garantir la sécurité de nos utilisateurs en dépit des nombreuses nouvelles habitudes d'utilisation? ». Pour y répondre, le système de sécurité Google s'étend aux objets connectés: chaque nouvel appareil Google requiert ainsi le même niveau d'authentification qu'un appareil traditionnel comme un ordinateur ou un téléphone, et son activité est suivie avec attention par les mêmes systèmes de détection des anomalies.



“ De nombreuses mesures de sécurité sont appliquées en arrière-plan ”

Mark Risher

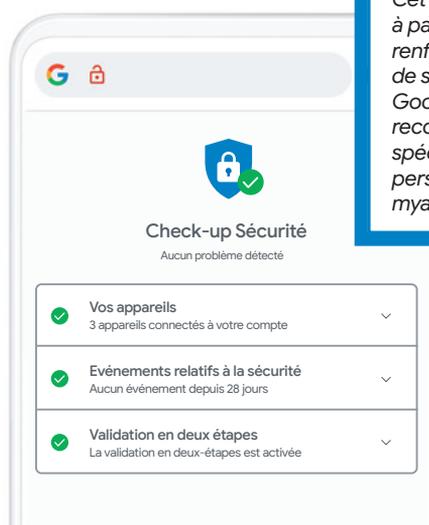
En quoi l'intelligence artificielle vous aide-t-elle à protéger vos utilisateurs ?

- **Mark Risher** : Nous l'utilisons pour Gmail depuis sa création. Supposons que plusieurs utilisateurs rencontrent des incidents suspects que nous ne pouvons pas classer: une machine à apprentissage automatique (une forme d'intelligence artificielle) peut comparer ces événements et, dans le meilleur des cas, reconnaître de nouvelles formes

d'escroquerie avant même qu'elles ne soient diffusées sur Internet. Mais tout n'est pas parfait. Alors que je travaillais pour un autre fournisseur de services de mails, un employé de banque nous a écrit depuis Lagos. À cette époque, les arnaques par mails qui provenaient supposément du Nigeria étaient monnaie courante et cet homme se plaignait que ses mails finissaient toujours dans le dossier spams alors qu'il travaillait pour une banque sérieuse. C'est ce genre de situations que l'intelligence artificielle nous aide à surmonter.

Check-up Sécurité

Cet outil guide pas à pas l'utilisateur pour renforcer la sécurité de son compte Google avec des recommandations spécifiques et personnalisées.
myaccount.google.com



Ok Google j'ai encore une question



Comment Google protège ses utilisateurs contre les attaques en ligne ?

Vincent Courson,

Responsable communication,
équipe Trust & Safety* de Google

C'est une question de couches de protection qui se superposent ! On commence par les protections qui sont incluses directement dans chaque produit et qui utilisent souvent les technologies les plus avancées, comme le "Machine Learning" (apprentissage automatique). Ces systèmes permettent par exemple de détecter et de bloquer automatiquement dans Gmail des centaines de millions de spams chaque jour ! Ensuite, il existe une couche de protection couvrant plusieurs services à la fois. Par exemple, Google Safe Browsing (navigation sécurisée) adresse des avertissements aux utilisateurs sur le point de naviguer sur des sites dangereux ou de télécharger des fichiers à risque, que ce soit sur Google Chrome, Gmail, le moteur de recherche, et d'autres services encore. Nous protégeons ainsi 4 milliards d'appareils. Enfin, la dernière couche de protection consiste à donner aux utilisateurs des outils pour qu'ils renforcent eux-mêmes leur sécurité en ligne. Ainsi, des technologies telles que l'authentification à deux facteurs ou le Programme Protection Avancée rendent le vol de compte Google bien plus complexe pour des acteurs malveillants.

Que faisons-nous pour vous protéger en ligne ? Que faisons-nous avec vos données ? Nos experts vous répondent.

Que fait Google avec les données des utilisateurs ?

Benjamin Amaudric, Directeur juridique adjoint de Google France

Les données que nous recueillons, comme les historiques de recherche et les vidéos regardées, sont destinées à améliorer nos services et l'expérience utilisateur. Google collecte aussi des données liées à la localisation pour fournir aux utilisateurs des résultats plus pertinents, comme un restaurant près de chez eux plutôt qu'à l'autre bout de la France. Bien entendu, en tant qu'utilisateur, vous gardez toujours le contrôle de vos données, en décidant par exemple de ne plus recevoir de publicités personnalisées ou d'effacer tout ou partie de vos historiques de recherche, selon les services utilisés (Google Maps, Google Search, YouTube, etc.). Google ne vend pas les données personnelles de ses utilisateurs. Notre priorité est d'intégrer la sécurité dans tous nos produits et services, que ce soit Gmail, le navigateur Chrome ou encore le stockage de données.

Comment Google anticipe les changements législatifs liés aux nouvelles technologies ?

Benjamin Amaudric, Directeur juridique adjoint de Google France

Google se conforme aux lois des pays dans lesquels il opère. Ceci étant, les nouvelles technologies évoluent très rapidement et l'on constate souvent que le législateur tend à faire voter une loi dès qu'un nouveau problème se pose. L'évolution rapide des technologies rend les nouvelles lois très vite obsolètes. La loi doit, selon nous, poser les principes à respecter, mais ne doit pas tomber dans l'écueil de l'abondance de détails, lesquels deviennent vite sans objet compte tenu de l'évolution des usages et des services sur Internet. Cela vaut dans tous les domaines, qu'il s'agisse de la lutte contre la haine en ligne ou de la protection des consommateurs. Google croit aussi beaucoup à la collaboration entre les différents acteurs et les gouvernements. Google soutient par exemple des initiatives comme le Global Internet Forum to Counter Terrorism, destiné à lutter contre le terrorisme en ligne, et a adhéré aux codes de conduite lancés par l'Union européenne pour lutter contre la haine en ligne et la désinformation.



Hackers en formation

Depuis 2008, une **formation unique en France** apprend aux étudiants à s'infiltrer dans des systèmes informatiques... pour mieux les défendre. Reportage en immersion.

Peut-on se défendre si on ne sait pas attaquer ?

La question résume à elle seule la philosophie des enseignements dispensés depuis 2007 à Maubeuge, en licence professionnelle CyberDéfense, Anti-Intrusion des Systèmes d'Information (CDAISI). Et la réponse, un « non » clair et sans appel, est donnée par Franck Ebel, 52 ans, responsable pédagogique à l'origine de la formation. « Nous apprenons à nos étudiants à attaquer les systèmes informatiques parce que c'est le seul moyen efficace d'en identifier les points faibles », détaille l'expert en cybersécurité, titulaire d'un DEA en électronique, qui regrette qu'on le considère parfois comme un « pirate ». « Nous enseignons des techniques de

hacking éthique, ce qui nous différencie des pirates informatiques. Nous avons recours aux mêmes techniques, mais notre but n'est pas de piller les informations des entreprises ni de les faire chanter, mais, au contraire, de leur venir en aide. » La formation CDAISI est scrutée de près par le monde professionnel, de plus en plus sensible aux questions de cybersécurité. « Nos étudiants trouvent tous un travail à la sortie de leurs études et il n'est pas rare qu'ils soient approchés en amont par des chasseurs de têtes », se félicite l'enseignant.

Le succès n'allait pourtant pas de soi. « Dans les années 2000, personne ne comprenait ce que l'on

“ Nos étudiants trouvent tous un travail à la sortie de leurs études ”

Franck Ebel

faisait en dehors des cercles d'initiés », se souvient avec un léger sourire le hacker en chef. C'est un événement bien précis qui va le pousser à créer une formation diplômante spécialisée. « En 2003, alors que j'enseignais en DUT informatique à Valenciennes, je me suis rendu compte que certains de mes étudiants tentaient de pirater le système informatique de l'établissement. Ils essayaient d'avoir accès à leurs notes pour les modifier. Je me suis alors demandé s'il existait une formation capable d'enseigner ce type de connaissances ? Et, bien sûr, la réponse était non. » Franck Ebel réunit ses amis, Robert Crocfer et Jérôme Hennecart, et, ensemble, ils décident de se lancer dans l'aventure.

La recherche avant l'attaque

Après des débuts tumultueux, tout bascule en 2010, lorsque la gendarmerie nationale les sollicite pour de la formation. Un gage de reconnaissance qui a changé la donne, et oblige également les formateurs à une grande prudence. Il faut dire qu'en 450 heures de cours, 100 heures de projet et 18 semaines de stage, les élèves en CDAISI acquièrent des compétences qui peuvent se révéler très sensibles. Robert Crocfer se charge par exemple de les former au travail d'enquête : « On appelle cela du profilage. Avant de mener une attaque, il faut impérativement acquérir une connaissance précise de l'environnement du système attaqué. Cela peut prendre des mois et nécessite de gros efforts de recherche. C'est une condition nécessaire à la réussite d'une attaque. » Son collègue Damien Bancal inculque, lui, les méthodes de “social engineering” aux futurs hackers éthiques. « Ces méthodes sont très éloignées de l'informatique et les élèves sont souvent surpris, observe Jérôme Hennecart,

professeur de sécurité des systèmes. Ils doivent apprendre à décrocher leur téléphone et à soutirer le maximum d'information à leur interlocuteur. Ce sont des méthodes employées dans 90 % des cyberattaques. » Avec l'accord des entreprises visées, les élèves apprennent aussi, par exemple, à prendre le contrôle d'un drone ou de barrières automatiques à l'entrée de parkings. L'équipe pédagogique veille donc particulièrement à ce que les règles “éthiques” soient bien intégrées par les étudiants : « Des cours de droit leur sont dispensés sur les procédures et les peines qu'ils encourent en cas de litige. Et, surtout, on leur fait comprendre qu'ils s'amuseront tout autant dans la légalité, en plus de très bien gagner leur vie ! », rassure Jérôme Hennecart.

Aujourd'hui, les étudiants planchent en cours de gestion et administration des systèmes, matière enseignée par Frédéric Vicogne. Leur mission : mettre en sécurité les machines. Installés à leurs postes de travail, ils échangent entre eux, à haute voix, dans un langage de spécialistes. Baptiste, 20 ans, a deux fenêtres de script noires ouvertes devant lui. Il vulgarise : « Je dois repérer les fichiers qui représentent les droits des administrateurs et utilisateurs, les lister, puis créer un script qui va permettre de vérifier de temps en temps que personne n'a tenté de les modifier. » Après une terminale S, Baptiste a enchaîné avec un DUT informatique à Maubeuge avant de rejoindre la licence pro. « J'ai toujours aimé fouiller dans les PC et comprendre comment cela fonctionnait. Il y a quelques années, j'ai poussé un peu plus loin et je me suis rendu compte du nombre de failles qui pouvaient exister dans les systèmes informatiques. Et honnêtement, ça fait peur ! C'est ce qui m'a motivé à entamer ce cursus », précise l'étudiant, qui souhaite poursuivre ses études au moins jusqu'à bac +5. « Je voudrais me tourner vers l'intelligence artificielle, parce que certains virus ont recours à des algorithmes, et je crois que réussir à lier cybersécurité et intelligence artificielle est un enjeu réel pour l'avenir », ajoute-t-il.

La plupart de ses camarades de classe poursuivront également leurs études jusqu'au bac+5. Certains deviendront “pentester” – spécialiste réalisant des tests d'intrusion sur un système pour s'assurer de sa sécurité –, un nouveau type d'expert que les entreprises s'arrachent. Seul regret partagé par l'ensemble de l'équipe pédagogique : le manque de femmes dans la promotion. « Nous recevons 500 candidatures chaque année et retenons 50 étudiants. Parmi les 500 candidats, 10 au maximum sont des femmes. Cette année, nous en avons retenu une », précise Franck Ebel, avant d'ajouter : « Nous n'avons jamais eu plus de deux filles par classe, mais chaque année, elles se positionnent en tête de promotion. C'est une particularité française : on pense que les filles ne sont pas faites pour l'informatique, mais c'est faux ! D'ailleurs, dans les autres pays, les filles sont beaucoup plus nombreuses à choisir ces filières. » Appel à candidatures...



En première ligne contre les cyberattaques

Face à des menaces en constante évolution,
Google développe des technologies de
pointe pour protéger les utilisateurs du
monde entier.



Les hackers ne s'intéressent plus - seulement - à des codes de cartes bancaires. Quelques heures avant les élections parlementaires néerlandaises de 2017, deux des plus importants sites d'informations sur les élections n'étaient plus accessibles, victimes d'une attaque DDoS ("Distributed Denial of Service Attack": attaque par déni de service, visant à saturer ou inonder un réseau de requêtes pour empêcher son fonctionnement). Le monde de la cybersécurité doit ainsi faire face à des menaces bien plus diverses et efficaces qu'auparavant. Si l'on en croit Guemmy Kim, experte en charge des initiatives sécurité chez Google : « *Le nombre d'attaques a augmenté et, dans le même temps, elles sont devenues plus complexes et sophistiquées. Dans le cas des attaques de masse, nous voyons des méthodes élaborées que nous avons rarement vues dans le passé* ». Le hacking s'est structuré et professionnalisé, loin de l'image caricaturale de l'adolescent solitaire œuvrant depuis sa cave. « *La plupart des hackers travaillent à présent en équipe et partagent des technologies*, reprend Guemmy Kim. *Dans de nombreux cas, ils sont également très bien formés et très bien financés. Mais nous pouvons nous adapter à cela. Les pirates informatiques changent constamment leurs méthodes et nous répondons en conséquence. Nous essayons également de travailler préventivement et de nous préparer aux nouvelles techniques qui ne sont pas encore répandues* ».

Une vigilance de tous les instants

Pour anticiper et contrer les attaques éventuelles, Google développe des technologies de pointe et met en place des processus méticuleux à tous les niveaux. L'attention portée à la sécurité remonte à

“ Nous répondons en conséquence et nous essayons également de travailler préventivement ”

Guemmy Kim

la phase de conception des produits : c'est le concept du "Privacy by Design"*.

Cette tâche complexe est sous la responsabilité d'une équipe dédiée de plusieurs centaines de personnes au nom digne d'une série : la "Night Watch" (Garde de Nuit). Et comme toutes les superteams dignes de ce nom, la Night Watch compte dans ses rangs un large panel de spécialistes, en cryptographie, biométrie, anonymisation des données ou encore intelligence artificielle, qui travaillent main dans la main avec d'anciens journalistes, activistes ou neuroscientifiques. La Night Watch est ainsi incluse dans tous lesancements des produits majeurs de l'entreprise. D'ailleurs, si le responsable de l'équipe considère que toutes les conditions essentielles de sécurité ne sont pas réunies, il peut même choisir de poser son veto. Pour limiter les failles potentiellement exploitables, les experts

Transparence des informations

Google publie régulièrement sur son site *Transparence des informations* (transparencyreport.google.com) les données qui révèlent comment les règles et les actions des autorités administratives et des entreprises affectent la confidentialité, la sécurité et l'accès aux informations. Une démarche permettant d'encourager les autres acteurs à adopter des normes de sécurité plus robustes, afin de rendre le Web plus sûr pour tous.

* Protection de la vie privée dès la conception



Programmes de récompense Google

En 2010, Google a lancé le "Vulnerability Reward Program" (VRP), un programme de récompense destiné à encourager les hackers à identifier des bugs dans ses services ou outils. « Nous avons besoin de talents externes pour chercher les failles là où l'on ne les attend pas forcément » explique ainsi Eduardo Vela, responsable de l'équipe de sécurité des produits Google. Plus récemment, en août 2019, le Data Protection Reward Program, programme dédié aux abus de données, a également été annoncé. Développé avec HackerOne, plateforme de référence, cette initiative a pour objectif d'identifier et de limiter les détournements de données dans les applications et les extensions Chrome.

en sécurité informatique du "Project Zero", fondé en 2014, traquent quant à eux les vulnérabilités qui n'ont encore aucun correctif connu, appelées "Zero Day Vulnerabilities" - d'où le nom de l'équipe. Celle-ci ne se limite d'ailleurs pas aux services de Google, mais à tous les logiciels impactant potentiellement leurs utilisateurs, du système d'exploitation au gestionnaire de mots de passe en passant par le service de messagerie. Par exemple, en mars 2017, une vulnérabilité dans un gestionnaire de mot de passe a été détectée : dans certaines conditions, le dernier identifiant utilisé pouvait fuiter à cause d'un cache non mis à jour. Cette faille a ensuite été corrigée par le fabricant avant d'être rendue publique.

Comme l'a prouvé l'exemple des élections néerlandaises, l'argent n'est pas toujours la motivation première des hackers. Pour répondre à ces nouvelles problématiques, il faut se tourner du côté de Jigsaw - Puzzle en français - centre d'innovation de la société mère de Google, Alphabet, où près de 60 employés œuvrent contre la censure sur Internet, les groupes radicaux ou encore pour protéger les personnes contre le harcèlement en ligne. Les équipes de Jigsaw ont, par exemple, développé "Project Shield", un système de protection dédié aux sites de journalisme indépendant ou ayant trait aux Droits de l'Homme

ou aux élections, ou encore "Perspective", un outil facilitant la modération, lancé en partenariat avec *Le Monde*, *New York Times*, *The Guardian* et *El País*. Grâce à l'apprentissage automatique, "Perspective" repère des récurrences dans les données pour identifier les injures ou le cyberharcèlement, et indique leur impact potentiel sur une conversation. Les éditeurs peuvent ensuite utiliser cette information pour interagir en temps réel et aider les modérateurs à trier les commentaires plus rapidement.

Evidemment, la sécurité est l'affaire de tous. Voilà pourquoi Google partage depuis longtemps ses connaissances, son expérience et ses technologies en matière de sécurité avec ses partenaires, ses concurrents et des organisations du monde entier. Face à une menace qui évolue, la collaboration continue de l'ensemble du secteur est essentielle pour faire progresser la recherche sur la sécurité, la confidentialité et la lutte contre les abus.

Facteur humain

Gilles Favier a fondé la société Encelis, qui utilise la psychologie cognitive pour sécuriser les systèmes informatiques. Il est convaincu que l'humain a un grand rôle à jouer dans la réduction du nombre de cyberattaques.



Quelles sont les failles humaines exploitées par les pirates ?

L'émotion en premier lieu, comme celle suscitée par un mail réclamant un don au profit d'une cause noble. L'appât du gain ensuite, parce que personne ne veut rater une bonne affaire.

Pourquoi sommes-nous insouciants sur Internet ?

L'outil informatique ne nous permet pas de constater les conséquences de nos actions dans le monde extérieur. En psychologie, cela se nomme la « perte du sentiment d'agentivité ». Lorsque l'on clique sur un lien malveillant, dans un mail ou une page web, nous ne voyons pas le virus qui s'installe. Alors on reste serein. Le psychologue Daniel Kahneman, Prix Nobel d'Économie, a théorisé le fonctionnement du cerveau sous la forme de deux « systèmes ». Le système 2 est lent, réfléchi, et nous sert pour les opérations complexes alors que le système 1 est rapide, émotionnel et incontrôlé. On l'utilise pour toutes les fonctions « automatiques », via des opérations mentales rapides pour apporter des réponses quasi-immédiates et donc plus sujettes aux erreurs. Or, l'outil informatique fait généralement appel à ce dernier.

Comment faire pour s'en prémunir ?

Il faut être plus vigilant. C'est compliqué car les pirates savent détourner notre attention. L'adresse mail est toujours savamment usurpée et le mail bien rédigé. Mais lorsque vous regardez bien, vous constatez que ce n'est pas le même nom de domaine ou qu'il y a des tournures mal formulées. Si votre caissier au supermarché vous demande votre numéro de téléphone ou vos clés, cela active notre vigilance. Vous devriez réagir de la même façon face à un écran. Mais un mail qui nous demande des informations personnelles n'active pas notre vigilance car nous sommes habitués à les donner pour s'inscrire ou payer, même sur des sites inconnus. L'usage du web et des mails, à l'usure, contourne les mécanismes cognitifs de vigilance et d'autant plus facilement qu'il ne s'agit pas d'interactions réelles. C'est la vigilance humaine couplée à la technologie qui permettra de sécuriser davantage notre environnement numérique.

Comment votre connaissance de la psychologie vous aide-t-elle dans votre approche de la cybersécurité ?

La norme sociale est un levier comportemental très intéressant en cybersécurité. Elle est basée sur les "nudges", des incitations destinées à orienter une décision sans l'imposer. À l'instar des messages affichés sur les panneaux d'autoroute : ils ne sont pas obligatoires mais le conducteur sait qu'il a à y gagner en les respectant. Nous avons appliqué ce mécanisme dans une entreprise qui avait été victime d'une attaque par "phishing" (hameçonnage). Nous avons communiqué à tous le nombre de personnes ayant eu un comportement inadapté, puis félicité ceux qui n'avaient pas cliqué sur le lien suspect et sensibilisé les autres. Comme personne n'aime être classé dernier, ceux ayant cliqué étaient conduits à faire évoluer leur comportement et la vigilance des autres était confortée. Le regard extérieur compte beaucoup dans notre inconscient. Un autre exemple est celui que nous appelons « l'option par défaut », notamment utilisé par les services de messagerie qui placent automatiquement les mails avec des liens potentiellement malveillants dans un dossier « indésirables ». Consulter un mail placé dans un tel dossier requiert un coût cognitif supérieur à l'ouverture quasi-automatique de ce même mail placé dans la boîte de réception classique. Le biais de « statu quo » entre alors en jeu : notre propension à maintenir la situation existante plutôt que de la changer. La sécurité se voit donc renforcée.

Le combat d'Eva

Trois à quatre fois par jour, son portable vibre. Elle peut fermer les yeux, soupirer, ça ne l'empêchera pas de vibrer. De nouveaux messages inconnus. Tous proviennent de femmes qui ont peur d'hommes, peur qu'ils aient piraté leurs téléphones, leurs ordinateurs, et qu'ils aient désormais accès à toute leur vie. « Entrer dans le téléphone de quelqu'un, c'est comme entrer dans son esprit », a l'habitude de dire Eva Galperin. D'après son expérience, les genres s'inversent parfois, mais l'immense majorité des "stalkers"* sont des hommes. Et une fois qu'ils ont "hacké"* les comptes ou les appareils de leurs victimes, ils savent tout. Eva, 40 ans, va tenter d'aider ces femmes.

« Il existe peut-être cent applications utilisées pour espionner des conjoints, pose-t-elle depuis son bureau de San Francisco. Elles viennent de partout dans le monde et elles sont constamment revendues, re-brandées... » Pourtant, elles ne sont pas nouvelles. Eva ne se souvient même plus quand elle a entendu parler pour la première fois des "spyware", aussi appelés "spouseware" ou "stalkerware"*. Peut-être autour des années 2000. « Ça se passe depuis des années, mais l'avènement des smartphones a aggravé la situation parce qu'ils sont partout et qu'ils contiennent énormément d'informations sur nous. Il est très tentant de les pirater. » Dans la plupart des cas, ce n'est pas même nécessaire,

les victimes ayant tout simplement donné leurs mots de passe à leurs anciens compagnons. « Parce que dans ce genre de relation toxique, ça se fait souvent », a constaté Eva. Les hackers ne sont pas toujours des anonymes œuvrant à l'autre bout du monde avec tout un attirail technologique, mais bien des proches ayant facilement accès à leurs cibles.

Eva aiguille comme elle peut ces femmes qui lui écrivent. « La première chose que je leur conseille, c'est d'essayer de faire la différence entre un compte compromis et un appareil compromis. Si ce n'est que le compte, il faut changer le mot de passe,

Elle ressemble à un petit lutin aux cheveux violets, surgi des méandres du Web pour venir en aide à ceux qui en ont besoin. Pour toutes les victimes de logiciels d'espionnage domestique, Eva est là.

en installer un qui soit unique et solide, rien qui puisse être deviné, même par quelqu'un qui les connaît bien, utiliser un gestionnaire de mots de passe et utiliser le plus possible l'identification à deux niveaux. Généralement, cela suffit. Mais si une femme continue de penser que l'homme qui la harcèle est encore et toujours au courant de choses qu'il ne devrait pas savoir, c'est probablement que son appareil, son téléphone ou son ordinateur est compromis. » Parfois il s'agit alors d'appeler un opérateur, de désactiver une webcam, de l'accompagner dans ses démarches. Parfois, seulement de la rassurer.

* "Stalker" : personne qui traque, piste, épie ou espionne - "Spyware, spouseware, stalkerware" : applications d'espionnage



“ Entrer dans le téléphone de quelqu’un, c’est comme entrer dans son esprit ”

Eva Galperin

« Être utile, efficace et respectueuse »

Cela fait un an que tout cela prend environ un tiers du temps d’Eva. À la fin de l’année 2017, elle découvre qu’un ancien collègue avec qui elle a travaillé pendant longtemps est accusé de viol par plusieurs femmes. Il se trouve qu’elles disent la vérité. « *J’étais très énervée, se souvient-elle. J’ai lu une*

interview de l’une des victimes à laquelle le journaliste demandait “Mais pourquoi ne pas avoir parlé plus tôt puisque c’était il y a longtemps ?”. Elle répondait qu’elle n’avait pas parlé parce que son agresseur était un hacker et qu’elle avait peur qu’il hacke son téléphone. J’ai trouvé ça terrible. » Eva ne veut plus que cette peur persiste et tweete : « *Si vous êtes une femme ayant été sexuellement abusée ou harcelée par un hacker qui a menacé de compromettre vos appareils, contactez-moi* ». Puis, elle va se coucher.

Le lendemain matin, son tweet a été partagé des milliers de fois. Son portable ne cesse de sonner. Un message à la fois, Eva essaie de tout lire, de tout comprendre, de tout absorber. « *J’avais déjà travaillé avec des gens*

abusés, notamment sur des terrains comme la Syrie. Mais jamais avec des victimes d’abus domestiques. Et, surtout, je n’avais jamais travaillé avec autant de victimes en même temps. » Eva se met à étudier « *la meilleure manière de s’adresser à elles, pour être utile, efficace et respectueuse.* » Il n’empêche que quand elle va se coucher le soir, les histoires tournent et retournent dans sa tête. « *Personne n’aime se réveiller le matin et, tout de suite, devoir lire les histoires les plus horribles* », observe-t-elle.

Une cause en héritage

Il était peut-être écrit qu’Eva Galperin finirait par défendre la vie privée, numérique ou non. Les histoires de sa famille juive ayant combattu les nazis en ex-URSS ont façonné sa vision de la liberté et de la conduite à adopter lorsque celle-ci est mise en péril, alors que son père, informaticien spécialiste de la sécurité, lui a donné le goût de l’informatique. De quoi faire d’elle une figure respectée. Dans les grandes conférences du monde entier, ses cheveux à la couleur changeante font toujours leur petit effet. Une façon comme une autre de capter l’attention une seconde de plus que les autres, et de s’y engouffrer pour faire passer son message.

Aujourd’hui, Eva est confiante. Si elle continue de recevoir des messages de femmes harcelées qui ont besoin de son aide, elle sent qu’au fond elle a déjà un peu gagné le combat des idées et de la morale. « *Ça prend du temps de changer les normes. Ce n’est que le début.* » Et les éventuelles menaces que cela aurait pu lui valoir ? « *Personne ne m’a jamais menacée directement, assure-t-elle en haussant les épaules. Sûrement parce qu’ils savent que ce serait une perte de temps.* »

Le jour où...

Ils sont responsables informatiques, créateurs YouTube ou encore critiques culinaires...
Quatre Français racontent le moment où ils ont compris l'importance de la sécurité en ligne.

Michaël

20 ans, créateur YouTube
Paris

Je fais des vidéos dans lesquelles je m'intéresse à l'informatique et à la cybersécurité. J'essaye de montrer aux gens quelles sont les bonnes habitudes à prendre, et à quel point ça peut être facile. Dans une vidéo en particulier, j'ai fait intervenir un spécialiste de la sécurité informatique. Le but c'était de voir, à partir d'une base de données d'utilisateurs qui avait fuité d'un site (ce qui arrive malheureusement fréquemment), si on pouvait « casser » les mots de passe. Il avait essayé plusieurs techniques et, pour faire court, sur les 50 000 mots de passe de la base de données, on en avait « craqué » près de 30 000, en quelques minutes. La démonstration était impressionnante. Et je me suis rendu compte qu'un mot de passe perçu comme fiable et fort par beaucoup d'entre nous, ne tient pas longtemps avec le bon matériel. Je ne pensais pas que ce serait aussi rapide. C'est sûr que si tu ne changes pas tes mots de passe après avoir vu ou vécu ça, c'est qu'il y a un souci. Il ne faut pas grand chose pour s'affranchir d'une bonne partie des problèmes, et ça permet de dormir un peu mieux.

Le conseil de Cybermalveillance.gouv.fr

Au regard du nombre important de mots de passe que nous devons utiliser, le plus simple est d'utiliser un gestionnaire de mots de passe. Il permet de les diversifier tout en respectant les bonnes pratiques.





Léo

Stéphane

47 ans, responsable
informatique
d'une structure associative
Rennes

Un jour de 2016, des collègues viennent me voir, paniqués : « On ne peut plus accéder à nos fichiers ! Qu'est-ce qui se passe ? » Après une analyse rapide, je remarque que toutes les extensions des fichiers (.doc, .xls, etc.) du serveur ont été changées par une autre extension que je ne connais pas. Il s'agissait en fait d'un "ransomware" : un logiciel malveillant qui exigeait une "rançon" pour déverrouiller nos fichiers. Cet événement a paralysé la structure et mes 15 collègues pendant une journée entière. Après une enquête approfondie j'ai compris que l'un d'entre eux avait cliqué sur une pièce jointe compressée dans un courriel vide... et le virus s'était propagé dans tout le serveur. Heureusement, j'avais des sauvegardes et j'ai pu rétablir les fichiers, mais cela a pris du temps.

Le conseil de Cybermalveillance.gouv.fr

Des sauvegardes régulières de ses données, dont on teste le bon fonctionnement, sont la meilleure protection contre les rançongiciels. Il suffira ensuite de réinstaller le système et les données.

33 ans, critique culinaire
Paris

C'était il y a quelques années. Je cherchais à acheter une affiche de la série X-Files en ligne pour décorer ma chambre. Je me retrouve par hasard sur un site allemand, un des seuls à en proposer. L'affiche coûtait 10 euros, je l'ajoute au panier et, au moment de finaliser le paiement, après avoir entré mes informations bancaires, je m'aperçois que les frais de port sont exorbitants, environ 15 euros. Je décide donc d'abandonner et je ferme la page. Une semaine plus tard, je vois une grosse somme prélevée sur mon compte, l'équivalent de 250 euros en pesos philippins. J'appelle mon conseiller bancaire qui m'indique qu'il s'agit d'un retrait effectué à Manille. Je n'ai pas trop de mal à lui prouver que j'étais à Paris à ce moment-là. L'assurance de ma carte bancaire m'a expliqué qu'il s'agissait d'une fraude exploitant les failles de sécurité de certains sites et happant les informations bancaires rentrées par les clients pour émuler la carte. La simplicité de l'opération m'a frappé. Je m'en suis aussi voulu d'avoir communiqué des infos aussi sensibles sur un site que je ne connaissais pas du tout. Je fais beaucoup plus attention depuis.

Le conseil de Cybermalveillance.gouv.fr

Il est préférable d'acheter sur un site basé en Europe et d'en vérifier la réputation. Une offre trop alléchante doit également inviter à plus de vérifications comme la lecture des mentions légales. Enfin, des systèmes de paiement à usage unique comme les e-cartes bleues sont à privilégier.

Stéphanie

42 ans, chef de projet
Strasbourg

Il y a deux ans, mon fils était en 4e. À la fin du premier trimestre, il a oublié de se déconnecter de son compte Facebook depuis un ordinateur du collège. Sauf qu'il ne me l'a pas dit tout de suite. Des garçons de sa classe en ont profité pour prendre possession du compte et ils ont commencé à envoyer des messages à ses contacts. Rien de bien méchant finalement, mais j'ai vu à quel point cela a atteint mon fils. L'autre problème était qu'ils avaient réussi à changer le mot de passe et que mon fils n'avait plus la main sur son compte. On a fait une réclamation et on a finalement pu le récupérer. Mais ça nous a fait prendre conscience à quel point des données et des discussions assez intimes peuvent tomber entre les mains d'autrui à cause d'une simple maladresse. Désormais mon fils comme moi vérifions bien que nous sommes déconnectés de nos comptes quand nous cessons d'utiliser un ordinateur public.

Le conseil de Cybermalveillance.gouv.fr

Il faut bien vérifier que l'on se déconnecte lorsque l'on a utilisé un appareil qui ne nous appartient pas. Le plus simple reste d'ouvrir un onglet de navigation privée et de le fermer à l'issue de la consultation de son compte. D'une manière générale, l'activation de la double authentification sécurisée de manière efficace l'accès au compte.



Une cyber journée à Rennes

Le programme **Google Ateliers Numériques** propose depuis 2012 des formations au numérique, en ligne ou dans des lieux dédiés. Comme à Rennes, où se déroulait une journée consacrée à la cybersécurité en septembre dernier.

L'exercice 11 est un véritable défi. Voilà bientôt quinze minutes que Stéphane n'a pas prononcé le moindre mot. Il s'éponge le front, pose ses yeux sur l'écran d'ordinateur et confesse en chuchotant : « *C'est comme si on me demandait de lire du chinois...* » Autour de lui dans la salle comble, tous sèchent sur cet exercice dit « fichier de sauvegarde », qui consiste à passer le barrage sécurité d'un document en trouvant son mot de passe caché. L'exercice 11 est la pièce maîtresse de l'initiation à la cybersécurité, imaginée par trois étudiants de l'école Epitech, baskets blanches, lunettes carrées et polos barrés du slogan « Cobra Coding Club ».

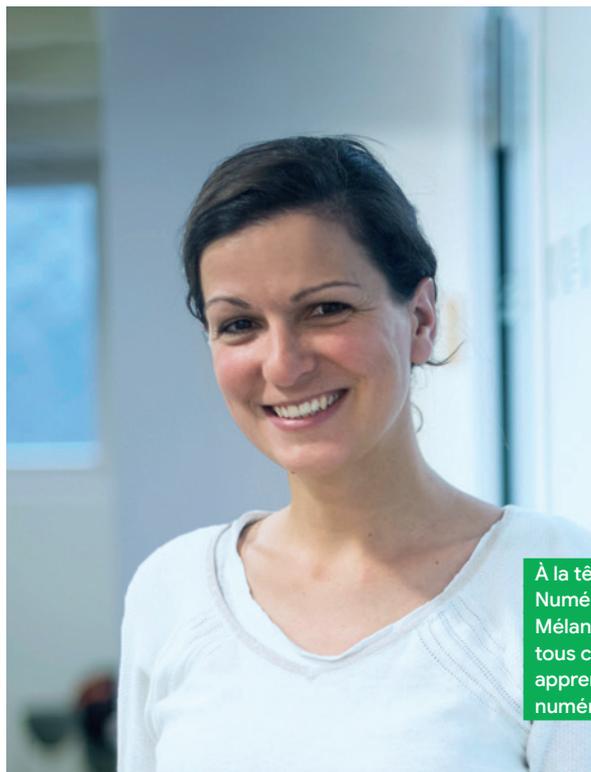
“ Les gens se retrouvent souvent face à des robots ou des répondeurs automatiques. Ici on rencontre une personne. ”

Mélanie Morin

Cette formation matinale lance la journée que l'Atelier Numérique de Rennes consacre à la cybersécurité. Pendant deux heures, chefs d'entreprise, demandeurs d'emploi, retraités, étudiants, ouvriers se sont glissés dans la peau de hackers pour mieux comprendre les dangers qu'ils pourraient rencontrer en ligne. Claire, 20 ans et animatrice de l'atelier, explique : « *Maintenant, les gens se rendent compte que des individus lambda peuvent récupérer des informations sensibles les concernant. On aborde cela sous la forme d'un jeu, mais la cybersécurité est la question la plus négligée depuis les débuts de l'informatique.* » À midi, après deux heures d'efforts, tous auront réussi grâce à l'accompagnement des étudiants. Félicien, chirurgien orthopédiste de 51 ans venu se former en vue de créer un site spécialisé, était pourtant novice en arrivant. Sac en bandoulière sur l'épaule, il glisse : « *Au début de ma carrière je ne savais pas comment marchait un bistouri, alors j'ai appris. C'est pareil!* »

Accompagner dans la durée

Aider le grand public à mieux maîtriser les outils numériques, tel est l'objectif majeur des Ateliers Numériques. « *C'est un enjeu vital,* souligne Mélanie Morin, en charge de la structure rennaise. *Il faut aider les gens dans cette transition numérique, notamment parce qu'un grand nombre de démarches se font aujourd'hui en ligne.* » Pour ce faire, Google propose des formations depuis 2012 – soit en ligne, soit à travers la France, dans les 200 villes visitées – qui ont déjà attiré plus de 400 000 personnes. Et pour aller encore plus loin, le premier Atelier Numérique a ouvert ses portes à Rennes, en juin 2018. S'en sont suivis Montpellier, Nancy et enfin Saint-Etienne. Une volonté de s'installer en « vrai », de s'inscrire dans la durée, comme le confirme Mélanie Morin : « *Les gens se retrouvent souvent face à des robots ou des répondeurs automatiques. Ici, on rencontre une personne.* » Gratuits et ouverts à tous, les Ateliers Numériques sont des lieux de partage proposant conférences, cours pratiques, rendez-vous personnalisés... Avec un accent mis sur le collectif : si la moitié des sessions est proposée par Google, l'autre moitié est assurée par des partenaires externes (associatifs, institutionnels ou privés). Si l'on en croit Mélanie Morin, la formule semble séduire une grande variété de profils : « *Nous accueillons aussi bien des structures associatives pour les enfants qui viennent s'initier au codage informatique que des personnes âgées, en passant par des professionnels, des personnes en recherche d'emploi ou en reconversion, des étudiants, des entrepreneurs porteurs de projets.* »

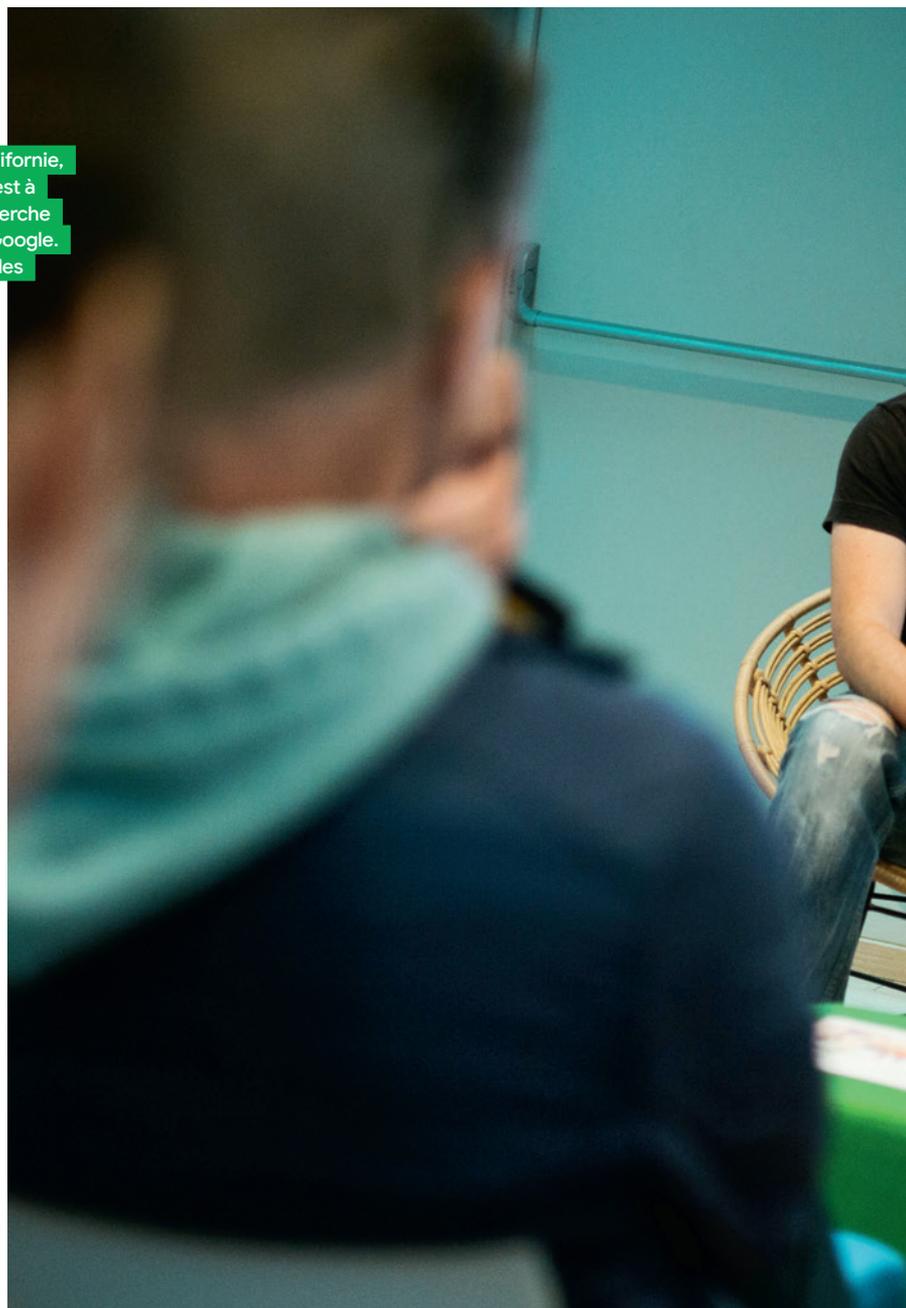


À la tête de l'Atelier Numérique de Rennes, Mélanie Morin accueille tous ceux désireux d'en apprendre plus sur le numérique.

Venu spécialement de Californie, le Français Elie Bursztein est à la tête de l'équipe de recherche sécurité et anti-abus de Google. Il est venu à la rencontre des professionnels rennais.

13h, place aux experts. Toutes les chaises ont trouvé preneurs, et même un peu plus : une trentaine de personnes issues du riche tissu rennais de startups, entreprises, laboratoires universitaires sont venues pour échanger avec l'un des plus grands experts en cybersécurité de la Silicon Valley. Elie Bursztein, béret à l'envers, est Responsable recherche sécurité & anti-abus de Google. Pour résumer, si des milliards d'utilisateurs gardent leurs comptes inviolés chaque année, c'est notamment grâce aux technologies que son équipe développe. Au milieu du grand salon de l'Atelier, meublé de poufs colorés et d'écrans tactiles muraux, le Français est venu présenter, l'espace d'une heure, « *un visage humain derrière Google* ». Vingt minutes de présentation et deux fois plus pour les questions-réponses, histoire de mieux comprendre les rouages, les aspirations et les positions de l'entreprise. « *La priorité numéro 1 de Google, c'est de préserver la confidentialité des données utilisateurs, qu'il s'agisse de Google Drive, Google Photos ou Gmail, énonce-t-il. Car les attentes vont vers plus de transparence : où vont mes données, comment sont-elles utilisées, comment sont-elles protégées ?* » Le public s'intéresse aux techniques mises en place, particulièrement à l'apprentissage automatique.

Pendant que la discussion se poursuit de manière plus informelle autour d'un buffet – l'occasion de poser quelques questions supplémentaires –, les participants de la formation de 14 h arrivent les uns après les autres, pas vraiment rebutés par la pluie qui s'est abattue à grosses gouttes. Intitulée « *Comment naviguer en toute sécurité sur Internet ?* » et agrémentée d'un complément axé sur les réseaux sociaux, cette formation est l'une des plus populaires selon Mélanie Morin, qui souligne l'augmentation



croissante de la demande sur le sujet depuis le début des années 2010, mais aussi le chemin qui reste à parcourir. « *Les gens n'ont pas toujours conscience que mettre une photo sur Internet veut déjà dire beaucoup de choses. Par exemple, un enfant qui fête son anniversaire, avec un gâteau où est inscrit son prénom et son âge, ce n'est pas anodin. En la postant sur Facebook, on donne son prénom, son âge, son visage. Il faut sensibiliser les enfants et les parents à cela.* » Chose faite avec Stéphane, heureux de pouvoir « *ramener à la maison des connaissances* » qu'il va transmettre à sa fille de 12 ans.



“ La priorité numéro 1 de Google, c’est de préserver la confidentialité des données utilisateurs, qu’il s’agisse de Google Drive, Google Photos ou Gmail ”

Elie Bursztein

« Parfois, on peut se sentir un peu seul sur Internet. Les gens qui viennent à ces conférences sur la cybersécurité me confient souvent qu’ils sont perdus quant à la protection de leurs données, et ils se demandent comment gérer cela de manière plus sereine. » Son leitmotiv : *« Répondre aux questions et, surtout, les amener à s’en poser d’autres. »* En une heure, Maryline aura appris à faire le diagnostic de son identité numérique à l’aide d’outils comme Google Alerts ou Deseat.me, mais également l’existence des recours à sa disposition, comme le règlement général sur la protection des données (RGPD) ou la Commission nationale de l’informatique et des libertés (CNIL). Elle est visiblement ravie : *« Ce que j’aime, c’est qu’on n’a pas l’impression de déranger les coachs avec nos questions. »* Elle reviendra.

Transmission

Maryline, professeure d’anglais retraitée de 63 ans, est venue assister à la conférence suivante – « Comment protéger ses données personnelles sur Internet ? » Elle avoue volontiers ses lacunes : *« Je suis venue pour m’améliorer un peu, sourit-elle. Il y a plein de choses que j’ignore. »* Quelques minutes plus tard, elle sèche ainsi sur le terme “cookies” et l’application Tik Tok. Rien d’inquiétant pour Léa Quéré, l’une des quatre animatrices formées sur plus de 35 thèmes et présentes en permanence à l’Atelier :

A portrait of Justine Atlan, a woman with long brown hair, wearing a dark top, looking directly at the camera with a slight smile. The background is dark and out of focus, showing some warm lights.

Naviguer, ça s'apprend

Comme un chant des cigales parisien, le clic-clac des claviers retentit dans la pièce aux hauts plafonds. Certains répondent au téléphone, chattent en ligne, d'autres forment de futurs formateurs. Le bruit de ses talons pressés sur le parquet la précède; la seconde suivante, elle vous accueille, volubile, en remuant les mains. Justine Atlan est la directrice générale de e-Enfance, association reconnue d'utilité publique, dédiée à la protection des enfants et adolescents en ligne. Ici, on aide, conseille et oriente de façon gratuite, anonyme et confidentielle, via le Numéro Vert national Net Écoute (0 800 200 000). Les "écoutants" ont ainsi reçu en 2018 les appels de 10 367 jeunes, victimes de cyberharcèlement, vol de données personnelles, usurpation d'identité ou encore "revenge porn" (vengeance pornographique), et qui n'ont pas forcément envie de parler des problèmes qu'ils rencontrent avec leurs parents.

« De la même façon que l'on est prudent dans la vie, il faut l'être sur Internet, ni plus ni moins »

Justine Atlan

Justine Atlan pose un diagnostic sans appel: le web n'est pas dangereux, c'est le monde qui l'est. « *De la même façon que l'on est prudent dans la vie, il faut l'être sur Internet, ni plus ni moins. Mais pour cela il faut savoir identifier les risques* », affirme-t-elle. Dans son bureau, un grand tableau aux airs de Basquiat 2.0, les collages de mains d'enfants et arobases en plus. « *Tout ce qui concerne l'enfant et le web, on est dessus* », sourit-elle. L'association s'est ainsi rendue indispensable depuis sa création en 2005.

Outre son travail de formation sur le terrain auprès des enfants, parents et professionnels, Justine Atlan saute désormais de rendez-vous dans les ministères en réunion avec les entreprises technologiques. Toujours dans le même but: protéger les mineurs. « *C'est ça notre ADN, travailler avec les pouvoirs publics et les industriels. Nous avons toujours eu cette volonté d'accompagner le développement du numérique en appelant à la vigilance pour les enfants.* » Et les challenges ne cessent d'évoluer.

En 2005, à la création de l'association, quels étaient les enjeux de la protection sur Internet ?

Ce n'était pas l'Internet d'aujourd'hui. Déjà, il n'y avait pas de smartphones! L'association s'est créée sur des questions simples: dans la vie, les enfants et les adultes sont traités de façon différente, à raison, alors pourquoi sur Internet, n'est-ce pas le cas? Comment

Depuis 2005, l'association e-Enfance accompagne enfants et adolescents pour qu'ils puissent profiter du meilleur du numérique et connaître ses limites. À sa tête, Justine Atlan, hyperactive et passionnée par les enjeux du numérique.

protéger nos enfants des dangers d'Internet, de contenus inappropriés ou de personnes mal intentionnées, tout en les laissant profiter de ce nouvel outil formidable ?

Alors, e-Enfance signe son "acte fondateur" : une charte entre les fournisseurs d'accès de l'époque et le ministère de la Famille, qui les engage à proposer à tous leurs abonnés un logiciel de contrôle parental gratuit. Mais un nouveau tremblement de terre se profile. « *En 2005, les jeunes étaient sur MSN et Skyblog. Mais en 2008, sont apparus en même temps Facebook, l'inventeur du réseau social, et le smartphone, cet outil très privé, très intime, que les jeunes gardent sous leur oreiller lorsqu'ils dorment. Ces deux nouveautés ont fait flamber les usages des ados et de nouvelles problématiques sont nées.* » Justine Atlan est alors repartie au combat. Ses armes : la pédagogie et le dialogue.

Aujourd'hui, les enfants sont nés avec le numérique. Quelle est la différence entre leur perception du Web et celle de leurs parents ?

Les enfants ne posent pas du tout les mêmes questions. Le numérique fait partie intégrante de leur vie depuis leur naissance. C'est une continuité de leurs vies « réelles », avec ce que cela implique par rapport à l'exposition de soi et la vie privée. Par ailleurs, l'instantanéité et la « gratuité » sont ainsi devenues la règle pour eux. Les parents en revanche, continuent d'avoir un regard plus distancié, et cela peut créer des difficultés de communication importantes. Ce sont deux représentations du monde, qui créent un fossé générationnel.

Quels sont les risques qu'ils encourrent à n'être pas assez prudent avec leurs données personnelles ?

L'enfant, par définition, est naïf. Il peut penser que c'est normal de pouvoir gagner des cadeaux sur le web. Alors ils jouent en offrant leurs données personnelles sans y penser. Il faut leur apprendre cette notion de données personnelles et son importance, ce qui revient à comprendre le modèle économique d'Internet. Nous expliquons à des enfants de plus en plus jeunes la notion de « gratuité » et ce qui est donné en échange. On leur apprend le ciblage publicitaire et leurs droits en matière de collecte des données personnelles.

Chez les ados, l'apprentissage est un peu plus complexe. « *Ce sont des consommateurs différents et ils ne voient souvent pas le problème*



à partager leurs données. Il fut un temps, avec les blogs et MSN, où le pseudo était la règle d'or, on pouvait dire à son enfant "Tu n'utilises que ton pseudo et tu ne donnes ton identité à personne." Mais Facebook est arrivé et a imposé la règle de l'identité réelle. Il est devenu normal de donner son nom sur le web. Il y a une éducation spécifique à développer, notamment sur le droit à l'oubli et le fait que les contenus vivent leur propre vie après avoir été postés. »

Encore plus difficile à expliquer : apprendre à garder certaines choses secrètes, pour eux qui partagent déjà tout, amitiés, amour, travail et photos. « S'il arrive parfois que leurs comptes de jeux en ligne soient piratés, c'est rarement le cas pour les réseaux sociaux. Ils ont plutôt été négligents en oubliant de se déconnecter ou en partageant leur mot de passe. C'est pour cela que nous leur apprenons à en changer régulièrement. Nous les comparons aux clés de chez soi qu'on ne laisse pas traîner. Car si on laisse sa maison ouverte, n'importe qui peut alors avoir accès à ses objets personnels. Voilà pourquoi on referme sa porte en partant. Le mot de passe, c'est personnel : on le garde pour soi. »

Comment faire, désormais, pour surveiller son enfant tout en instaurant une relation de confiance ?

Bien sûr, on ne va pas traiter un enfant de 9 ans comme un ado de 14. Plus tôt vous aurez transmis des règles et accompagné votre enfant, plus vous serez rassuré sur sa capacité d'autonomie en grandissant. Il y a par exemple le contrôle parental, qui peut aider à sécuriser l'environnement numérique. Mais un adolescent aura plus de mal à supporter un environnement filtré. Quoi que les parents choisissent, il ne faut surtout pas le cacher et être transparent, sinon l'enfant ira encore plus loin dans la dissimulation. La confiance, cela se partage.

Depuis plus de dix ans, plus d'un million d'élèves dans 10 000 établissements ont pu bénéficier des conseils et des ateliers de l'association. « Google fait appel à notre expertise depuis de nombreuses années, rapporte Justine Atlan. Fort de cette expérience, Google.org a choisi de nous soutenir dans la création d'un programme de prévention pour les primaires, car les enfants sont de plus en plus tôt sur Internet. » C'est la naissance des Super-Héros du Net. Une imagerie qui fonctionne bien avec les 8-10 ans, ravis de se voir attribuer des superpouvoirs et de ramener à la maison des Incollables® et des BD racontant les aventures de Ben et Lila, alias Netboy et Webgirl. Et si jamais cela peut influencer les parents... « Comme on l'a vu avec le tri des déchets, les enfants sont d'excellents prescripteurs de pratiques responsables. Ils sont soucieux de faire respecter par leurs parents à la maison les règles qu'ils ont apprises à l'école », souligne Justine Atlan.

Dans la pièce voisine, une formation se termine. On prépare les prochaines interventions en milieu scolaire. Les claviers chauffent toujours. Les téléphones sonnent. Justine Atlan est confiante. Les enfants apprennent vite, et les parents finiront bien par les rattraper. « Dans dix ans, les nouveaux parents auront eux aussi grandi avec le numérique. Ils se sentiront plus compétents et plus légitimes pour intervenir et encadrer leurs enfants en toute connaissance de cause. » En attendant, il y a Les Super-Héros du Net... et ceux d'e-Enfance.

“ Le mot de passe, c'est personnel : on le garde pour soi ”

Justine Atlan

Pour accompagner les familles en ligne, e-Enfance participe à la tournée nationale « Sécurité en Famille » initiée par Google dans 20 villes à partir de l'automne 2019.





Google Ireland Limited,
Gordon House, Barrow Street,
Dublin 4, Irlande

Numéro d'enregistrement : 368047
Numéro de TVA : IE6388047V
Ceci est une communication
de Google.

Directeur de la publication
Raphaël Goumain

Conception et réalisation
TBWA \ Corporate

Comité de pilotage
Raphaël Goumain
Hélène Marlaud
Sabrina Moualfi Belhmane

Directeur de la rédaction
Charles Alf Lafon

Comité de rédaction
Hélène Coutard, Gino Delmas,
Guillaume Depasse, Théo Denmat,
Maxime Jacob, Lucas Minisini

Responsable d'édition
Amina Chenoune

Chargée d'édition
Christine Nazon

Secrétariat de rédaction
Le Bureau des SR

Traduction : Lexcelera

Direction de création
Denis Deschamps

Direction Artistique
Manon Berge

Conception graphique
Annabel Deschamps

Iconographie : Fériel Simon

Illustration
Pat Grivet, Getty Image

Crédits photo
Julien de Rosa,
Guillaume Depasse, e-Enfance,
Getty Image, Google, Matt Mirniaga,
Conny Mirbach, Kelly Serre

Fabrication : EG+ Worldwide

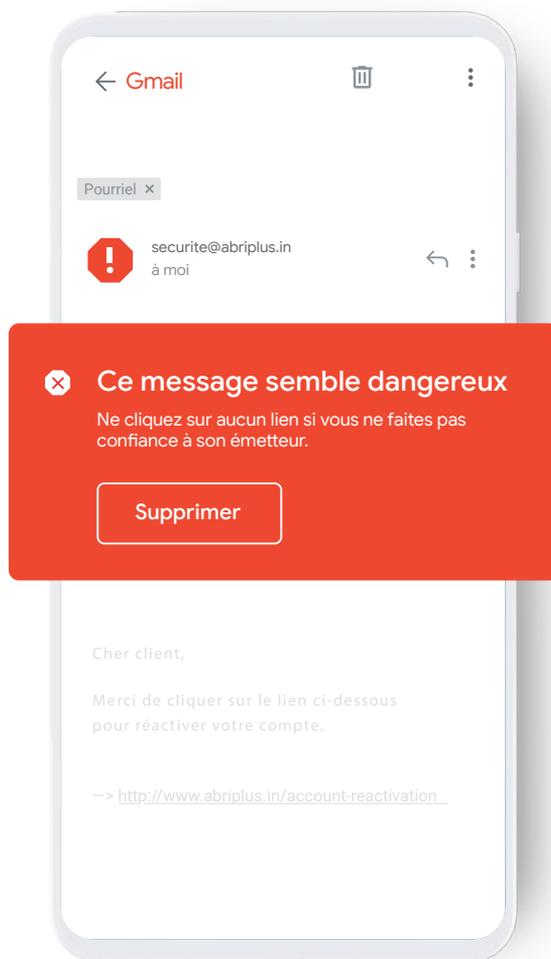
Remerciements

La rédaction souhaite remercier chaleureusement toutes les personnes qui ont rendu possible ce premier numéro d'Azerty. Et plus particulièrement : Olivier Esper, Amandine Guay, Arnaud Lecarpentier, Mélanie Morin, Charlotte Radvanyi, Line Zouhour Adi.

ISSN : en cours
Dépôt légal : à parution



Nous bloquons
plus de
100 millions
de tentatives
d'hameçonnage
chaque jour.



Grâce à l'apprentissage automatique, Gmail empêche 99,9 % des tentatives d'escroquerie (ou hameçonnage) d'atteindre votre boîte de réception. De cette manière, Google assure la confidentialité et la sécurité de vos informations personnelles.

g.co/centredesecurite

