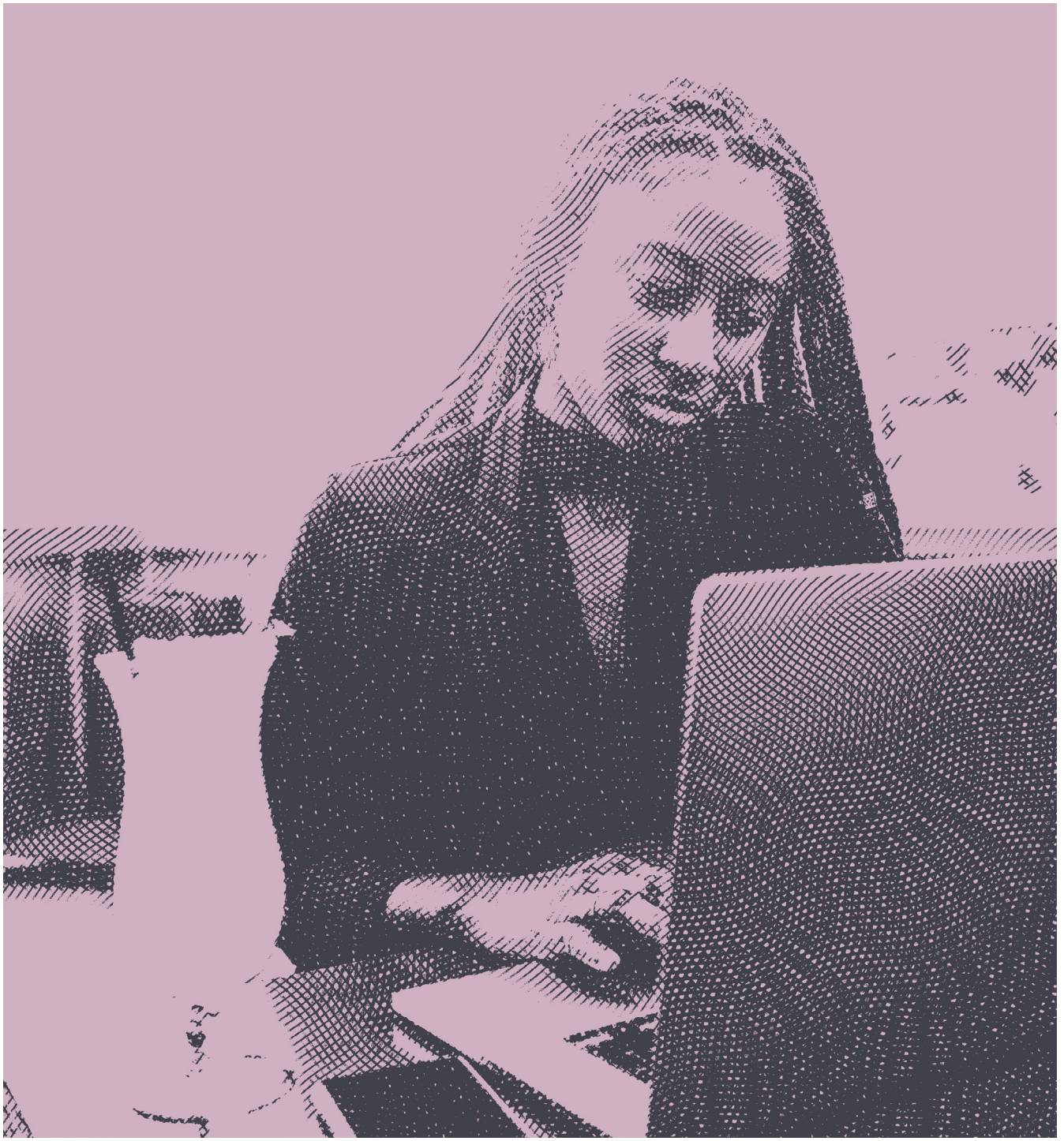
Digital Trust Index, Okta

Focus sur la confiance des Français dans le numérique



okta

Sommaire

> Le trop de confiance attire le danger.
>
> Pierre Corneille

Introduction

Les événements de 2020 ont placé la notion de confiance au centre de nos vies. Avec la pandémie, la confiance envers les gouvernements et institutions est devenu un sujet crucial pour la plupart des gens. Dans un climat de forte récession économique, la confiance des clients a fortement impacté les résultats financiers de la plupart des marques. En outre, de nombreuses organisations ont dû surmonter des réticences tout en devant permettre à leurs salariés de travailler depuis leur domicile, et faire confiance aux canaux numériques comme unique solution pour répondre aux besoins de leurs clients.

La pandémie intervient dans un contexte où les préoccupations relatives à la sécurité vont croissantes. Ce phénomène est notamment dû à des volumes de fuites de données et à des cybermenaces sans précédent, à la mise en application rigoureuse de réglementations sur la protection des données, et aux attentes grandissantes de la part des consommateurs en matière de confidentialité.

Pour les entreprises, la sécurité passe avant tout par la confiance. Pour mettre en place une sécurité efficace, elles doivent d'abord identifier quels niveaux d'accès donner à leurs employés, partenaires et clients, aux systèmes et données sensibles au-delà du périmètre physique traditionnel de l'organisation. Mais l'inverse s'applique également : la confiance passe d'abord par le sentiment de sécurité. En d'autres termes, la meilleure façon de gagner la confiance de ces acteurs clés est de proposer des outils et des politiques de sécurité efficaces – en particulier pour fournir une gestion transparente des identités des utilisateurs.

Cette approche constitue en effet le moyen le plus rapide pour accroître la productivité, fidéliser et renforcer l'engagement des employés, partenaires et clients.

Okta a réalisé une étude auprès de plus de 13 000 employés de bureau – dont plus de 1 000 en France – afin de mieux comprendre :

À quel point le monde du numérique contribue-t-il à inspirer, entretenir ou, à l'inverse, à dégrader la confiance ?

Quel est l'impact des interactions, désormais quasiment à 100% de manière digitale, sur la confiance ?

Les marques, entreprises et organismes gouvernementaux en font-ils assez pour renforcer la confiance ?

Quels facteurs externes affectent notre propension à faire preuve de confiance via des canaux numériques ?

Méthodologie

Sauf mention contraire, l'intégralité des chiffres provient de YouGov Plc. L'échantillon était composé de 13 163 employés de bureau du Royaume-Uni, des États-Unis, d'Australie, d'Allemagne, de France, d'Italie, d'Espagne, de Suède, des Pays-Bas et du Japon. L'étude a été réalisée en ligne du 26 novembre au 10 décembre 2020.

Ce rapport restitue l'Indice de confiance numérique d'Okta et cherche à explorer le principe de confiance dans un monde toujours plus transformé par les effets de la pandémie. L'analyse se conclut par des recommandations pour les particuliers, entreprises et organisations du secteur privé quant aux stratégies pouvant être adoptées pour inspirer et bâtir une confiance réelle du point de vue humain.

Partie 1

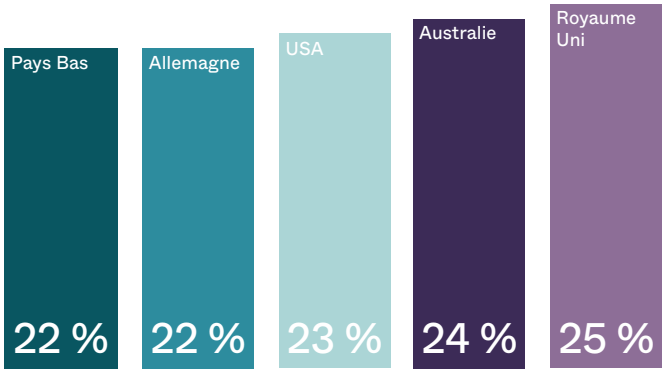
Pourquoi les consommateurs font-ils confiance aux marques ?

Avec l'avènement du télétravail en 2020, les employés de bureau ont passé beaucoup plus de temps sur leur ordinateur et ont aussi dépensé beaucoup plus d'argent en ligne.

L'année 2021 étant une année de transition vers des pratiques en ligne plus institutionnalisées, les marques doivent désormais bâtir de nouveaux modèles axés sur la confiance et la fidélisation avec toutes les parties prenantes.

La confiance ne se gagne pas facilement de nos jours. Cependant, bien que les valeurs éthiques soient de plus en plus valorisées par les actionnaires, les investisseurs et les conseils d'administration, il apparaît que les fondamentaux sont bien plus importants aux yeux des clients. La sécurité est également un paramètre essentiel. Ainsi, 17 % des répondants estiment que la mise en place d'options de connexion sécurisée (à l'image de l'authentification multifactorielle, ou MFA) et d'autres mesures permettrait d'entretenir la confiance vis-à-vis de ces marques. Ce ressenti est également fort en Australie (24 %), aux États-Unis (23 %), en Allemagne (22 %) et aux Pays-Bas (22 %).

32 % des personnes interrogées en France estiment que la fiabilité du service client est le critère le plus susceptible de leur inspirer confiance dans une marque digitale (par exemple lorsque celle-ci s'assure que les articles arrivent dans les délais et dans de bonnes conditions).



Pourcentage des personnes interrogées qui pensent que des options de connexion sécurisées telles que l'authentification multifacteur (MFA) contribueraient à entretenir la confiance vis-à-vis des marques.

L'impact des failles

Mais cela ne signifie pas que l'éthique n'a aucune importance : 8 % des personnes interrogées en France considèrent ce facteur comme le plus important pour inspirer la confiance. Ce paramètre joue également un grand rôle dans les prises de décisions lorsqu'il concerne les marques à exclure, en particulier concernant leur « éthique en matière de gestion des données ».

23 % Les principaux facteurs susceptibles de pousser les répondants français à se méfier d'une marque sont l'utilisation intentionnellement abusive ou la vente de leurs données personnelles ou encore l'erreur de commande.

Les expériences peu engageantes ou les erreurs sont également les plus fréquemment citées en Espagne (21 %) et en Suède (16 %).

En plus de constituer des problèmes sur le plan de l'éthique, ces pratiques sont également réprimandées par l'organisme de contrôle du RGPD en France, la CNIL. Ainsi, pour échapper à la colère de leurs clients, s'éviter de lourdes conséquences pécuniaires et protéger leur réputation, les organisations doivent s'assurer que les données qu'elles possèdent bénéficient d'une sécurité optimale grâce à l'adoption de meilleures pratiques de gestion des identités.

L'utilisation abusive ou la vente de données apparaissent également comme les principaux facteurs incitant les consommateurs à se méfier d'une marque dans l'ensemble des autres pays de l'étude. En Australie (16 %), aux États-Unis (15 %) et aux Pays-Bas (13 %) les fuites de données représentent la 2e principale préoccupation des répondants. Tout ceci sonne comme un rappel : bien que l'éthique en matière de traitement des données relève de la plus haute importance, la perfection en matière de service client ne doit pas être oubliée.

Quand la confiance est détruite

Dans l'environnement professionnel extrêmement compétitif d'aujourd'hui, il est clair que la confiance est un élément essentiel dans la réussite des marques.

78 % En France, 78 % des répondants n'effectueraient pas d'achats auprès d'une entreprise ne leur inspirant pas confiance.

41 % se méfieraient sérieusement des sites dont ils n'ont jamais entendu parler auparavant.

Sans surprise, les marques doivent redoubler d'efforts pour conserver la confiance des consommateurs.

Et pour ce faire, il est essentiel de mettre en place une cybersécurité efficace. En France, près d'un répondant sur quatre (37 %) affirme ne plus avoir confiance en une entreprise ou une marque suite à une fuite de données ou un événement similaire, et ce pourcentage est encore plus élevé aux États-Unis (56 %) et en Australie (40 %). Près de la moitié (43 %) des utilisateurs français ont définitivement arrêté de recourir aux services de telles sociétés, et 38 % d'entre eux ont supprimé leur compte.

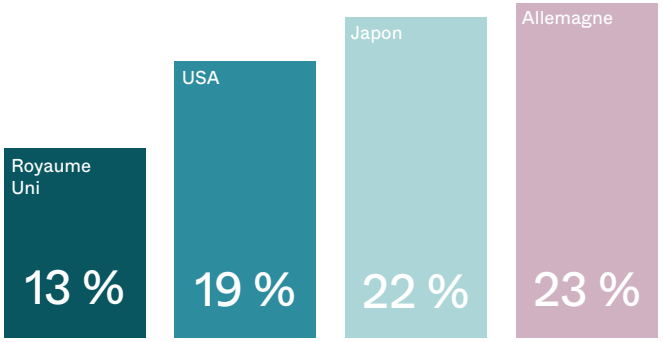
Fait notable : les jeunes français tolèrent encore moins que leurs aînés la mauvaise gestion de leurs données et les lacunes en matière de sécurité. Ainsi, 50 % des 18-24 ans affirment avoir totalement cessé d'utiliser les services d'une entreprise à la suite d'une faille, contre 42 % des 35-44 ans. Étant donné que les jeunes générations représentent le moteur de l'économie de demain, les marques doivent s'assurer que leurs priorités stratégiques soient alignées sur ces attentes accrues en matière de sécurité.

Étant donné que les jeunes générations représentent le moteur de l'économie de demain, les marques doivent s'assurer que leurs priorités stratégiques soient alignées sur ces attentes accrues en matière de sécurité.

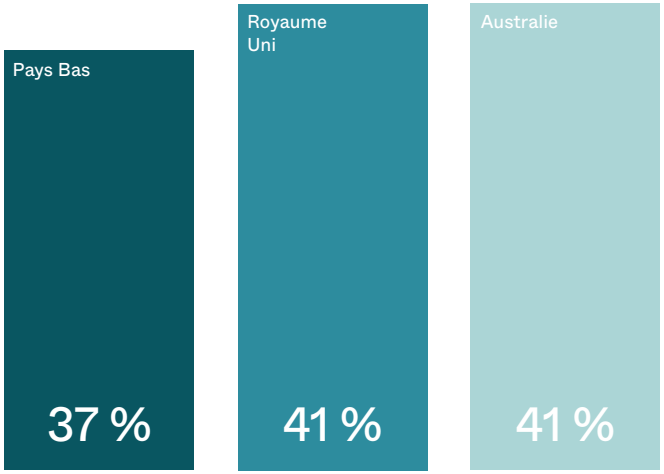
> Les plus jeunes générations deviendront les décideurs de demain. Les entreprises doivent donc s'assurer d'être bien préparées et de leur garantir une qualité de service et une cybersécurité optimales, afin d'aligner leurs priorités sur les besoins de leurs clients.
>
> Nicolas Petroussenko, Country Manager, Okta France

Encore beaucoup de travail à accomplir

En effet, 15 % de personnes interrogées en France estiment qu'aucun canal numérique n'est en mesure de garantir le traitement sécurisé de leurs données (ils sont 23 % en Allemagne, 22 % au Japon et 19 % aux États-Unis). A noter que les applications de communication professionnelles (9 %) sont considérées comme un peu plus fiables que les applications personnelles (7 %).



Pourcentage des personnes interrogées qui ne font confiance à aucun canal numérique pour gérer leurs données.



Pourcentage des personnes interrogées qui pensent que les sites web gouvernementaux sont les plus dignes de confiance.

En France, ce sont les sites web gouvernementaux qui inspirent le plus confiance (34 % des répondants). Cette impression est également partagée en Australie (41 %) et aux Pays-Bas (37 %).

Ces résultats sont indubitablement une chose positive. Malgré des inquiétudes initiales concernant le traitement des données personnelles et le COVID-19, aucune faille majeure n'a été rendue publique à ce jour. En outre, la vigilance constante semble contribuer au renforcement des standards en matière de sécurité des données.

> Le fait que les individus se fient aux sites gouvernementaux plus qu'à tout autre canal pour traiter leurs données est une excellente chose. Il est important pour ces organismes de continuer à donner la priorité aux mesures de cybersécurité et à la protection des données des citoyens.
>
> Nicolas Petroussenko, Country Manager, Okta France

Partie 2

Comment la pandémie a changé les comportements des utilisateurs

29% Près d'un tiers des Français (29%) déclarent travailler « souvent » ou « toujours » de leur domicile. Ces employés auront besoin de davantage de flexibilité au niveau des politiques de télétravail une fois la crise actuelle terminée.

Cependant, isolés chez eux, beaucoup se sont retrouvés exposés à l'augmentation de cyberattaques visant à dérober leurs identifiants professionnels et autres données relatives à leur identité personnelle.

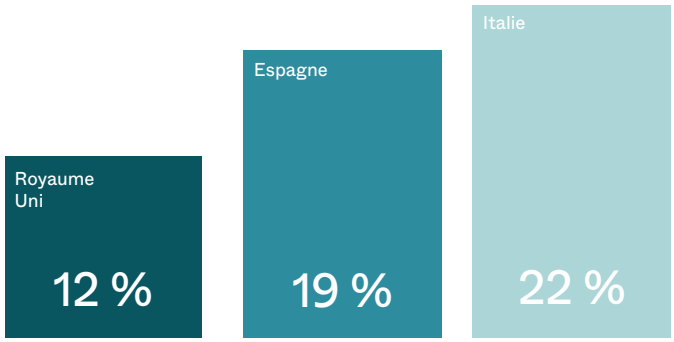
Le phishing, ou hameçonnage, est ainsi devenu la tactique préférée de nombreux cybercriminels en 2020. Ces derniers ont rencontré un grand succès en appâtant les individus avec des informations sur les vaccins, sur la COVID-19, ou avec de fausses nouvelles de dernière minute semblant provenir d'institutions dignes de confiance telles que l'OMS pour pousser les destinataires au clic. **En avril dernier, Google a annoncé** avoir bloqué 18 millions de logiciels malveillants et d'e-mails de phishing liés à la COVID-19 par jour.

Il n'y a donc rien de surprenant dans le fait que 42 % des français affirment être devenus plus prudents en renseignant leurs informations personnelles en ligne (seul 2 % d'entre eux le seraient moins aujourd'hui qu'auparavant).

Le télétravail a également rendu les répondants plus méfiants vis-à-vis des e-mails de phishing (45 %), des fuites de données (41 %) et même des deepfakes (ou « hypertrucages ») générés par des intelligences artificielles et utilisés pour diffuser de fausses informations (39 %).

21% Dorénavant, pour les répondants, le principal risque est celui de l'usurpation d'identité (21 %), ce qui est compréhensible compte tenu de la hausse des attaques de phishing à laquelle nombre d'entre eux été confrontés.

Les logiciels malveillants (17 %) et les fuites de données (14 %) complètent le podium des principales préoccupations.



Pourcentage des personnes interrogées qui pensent que le vol de mot de passe pose un problème.

Enfin, bien que le vol de mots de passe inquiète peu les employés de bureau Français (12 %), les Italiens (22 %) et les Espagnols (19 %) se sentent bien plus vulnérables face à ce risque, ce qui montre la nécessité de mettre en place des systèmes d'authentification renforcée.

En outre, il est important de garder en tête qu'un individu peut être exposé à des cybermenaces liées à des attaques le ciblant lui et ses appareils personnels, mais aussi à cause des agissements risqués en ligne de la part de personnes utilisant le même réseau Wi-Fi, par exemple.

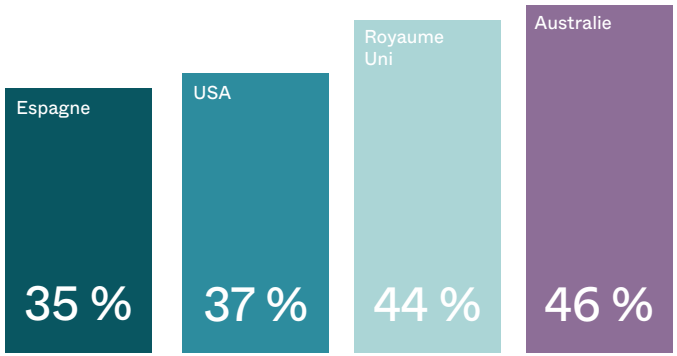
« L'exposition des employés en situation de télétravail s'est considérablement accrue pour des raisons multiples et complémentaires. Les employés se sont retrouvés à partager des appareils et à travailler sur des réseaux Wi-Fi domestiques moins sécurisés, augmentant ainsi les risques et compromettant la confidentialité de documents partagés ou d'appels passés.

Désormais, nous partageons notre espace de travail avec notre famille ou des colocataires, sans pouvoir bénéficier de la sécurité d'un service de proximité de nos collègues et du service IT. De plus, les réflexes en matière de cyber hygiène des employés peuvent désormais être inconsciemment compromis du fait de la frontière quasi-inexistante entre vie professionnelle et personnelle.

Ben King, CSO EMEA, Okta

L'heure est à la transparence

Depuis la pandémie, les Français sont devenus beaucoup plus méfiants et recherchent davantage d'informations sur la collecte de données ou les conditions générales (26 %). En revanche, c'est la couverture médiatique relative aux menaces en ligne qui vient en tête en Australie (46 %), aux États-Unis (37 %) et en Espagne (35 %).



Pourcentage des personnes interrogées qui pensent que la couverture médiatique des menaces a accru leur prudence en ligne pendant la pandémie.

S'il est remarquable de voir les journalistes jouer leur rôle dans l'information du grand public, les marques ont néanmoins elles aussi une excellente opportunité d'accroître la sensibilisation de leurs clients sur ces sujets, et ainsi d'inspirer davantage confiance. En associant ces efforts à des outils d'authentification multifactorielle, par exemple, elles peuvent offrir davantage d'assurance à des consommateurs inquiets, accroître ainsi leurs revenus et se distinguer de la concurrence.

De même, les employeurs ont également un rôle à jouer. En augmentant leurs efforts en matière de sensibilisation, en mettant à jour les technologies susceptibles d'être vulnérables aux menaces en ligne, et en démontrant l'efficacité des mesures de sécurité mises en place (à l'image de solutions de gestion des logiciels malveillants sur les terminaux), ils peuvent rassurer leurs salariés quant à leur protection, à domicile comme au bureau. Ces initiatives profiteront aussi bien indirectement aux marques digitales tierces qu'à leur propre organisation : en effet, le fait de renforcer la confiance vis-à-vis des outils utilisés par leurs employés pour le télétravail permettra à terme d'accroître leur productivité.

Partie 3

Comment les entreprises s'organisent-elles ?

Beaucoup d'employeurs ont effectivement pris des mesures pour lutter contre la montée des cybermenaces auxquelles sont confrontés les télétravailleurs. La mise en place de nouvelles applications et technologies de sécurité, à l'image de l'authentification multifactorielle, a été la mesure la plus populaire (30 %), suivie par l'amélioration des formations accessibles au personnel (22 %). Les deux sont essentielles pour inspirer le genre de confiance sur laquelle s'appuient les entreprises prospères.

Cependant, il est plus inquiétant de constater que près d'un quart des répondants (22 %) estime que leur employeur n'a rien fait jusqu'ici pour lutter contre la prolifération des menaces en ligne liée à la pandémie. Ce pourcentage est particulièrement élevé dans les secteurs de l'art et du divertissement (35 %), de l'immobilier (32 %) et de l'éducation et du juridique (29 %).

«

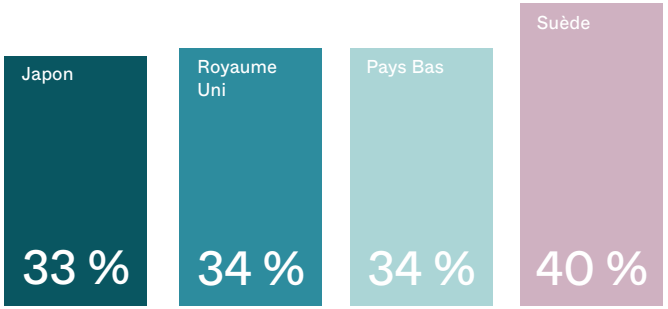
Dans les secteurs d'activités qui n'ont pas accompli leur transformation digitale, les employés se retrouvent souvent à travailler à partir d'environnements techniques moins évolués et n'ont souvent pas la connaissance ou les réflexes pour se protéger des menaces en ligne. Les secteurs qui ont traditionnellement toujours dû faire face à davantage de cyberattaques comme les banques, le secteur tech et la vente ont probablement bénéficié d'un budget de sécurité proportionnellement plus important.

Dans tous les secteurs, les DSI et les CISO ont dû répondre à la fois à des besoins nouveaux, spécifiques à chaque secteur et des projets de sécurité, souvent deux tâches très différentes.

Ben King, CSO EMEA, Okta

Pire, un quart des employés de bureau affirment ne pas savoir si leur employeur a pris des mesures proactives en matière de sécurité. Ce sentiment est encore plus fort chez les personnes interrogées en Suède, au Royaume-Uni, aux Pays-Bas ainsi qu'au Japon (respectivement 40 %, 34%, 34 % et 33 %).

Ces résultats sont particulièrement décevants, car ils sont un révélateur du manque de transparence entre les dirigeants, les responsables informatiques et les employés. Peu importe que l'on mette en place les meilleurs systèmes de sécurité au monde : si les salariés n'en savent rien, l'entreprise ne sera pas en mesure d'instaurer un climat de confiance avec son personnel.



Pourcentage des personnes interrogées affirmant ne pas savoir si leur employeur a pris des mesures proactives en matière de sécurité.

> Les cybercriminels trouvent constamment de nouvelles ruses et les professionnels le savent : beaucoup d'entre eux sont de plus en plus prudents face aux risques que représentent le phishing, les fuites de données ou encore les deepfakes. Les entreprises doivent donc s'assurer de garder une longueur d'avance et de lutter contre ces nouvelles menaces en adoptant de nouvelles approches.
>
> Nicolas Petroussenko, Country Manager, Okta France

Il apparaît clairement que les responsables informatiques doivent commencer à déployer des solutions basées sur une gestion souple des identités en fonction des risques (s'ils ne l'ont pas déjà fait), afin de proposer une sécurité reposant sur la confiance en 2021, d'accroître la productivité de leur personnel et de minimiser les cyber risques. En outre, ils doivent faire preuve de davantage de transparence quant aux nouvelles technologies et aux politiques de sécurité.

Partie 4

Conclusion et recommandations

IDC définit la confiance comme la condition qui « favorise la prise de décisions entre deux entités ou plus, et qui reflète le niveau d'assurance qui règne entre elles ». En outre, ce paramètre permet d'« élever les débats en matière de sécurité afin d'inclure des paramètres tels que les risques, la conformité, la confidentialité et même l'éthique professionnelle ».

Aucun responsable informatique ou dirigeant ne peut plus ignorer ce concept aujourd'hui, étant donné que les transformations numériques actuelles offrent de nouveaux canaux pour interagir avec ses clients et soutenir ses employés, mais elles augmentent aussi l'exposition aux cybermenaces. Abordée correctement, la confiance permet non seulement de limiter les dégâts, mais également aux organisations de créer de nouvelles opportunités de croissance et de la valeur ajoutée.

Dans l'entreprise, cela commence par l'adoption d'une approche Zero Trust axée sur l'identité, par la mise en place de politiques de gestion des accès basés sur les risques, d'authentification en continu et adaptative, et d'une gestion des accès sans accroc.

La pandémie a rendu la nécessité de telles approches encore plus urgentes. Les organisations doivent en effet pouvoir vérifier l'identité de leurs utilisateurs distants, les imposteurs étant toujours plus nombreux à tenter d'infiltrer les réseaux professionnels. Il est également important d'inspirer confiance aux employés afin que ceux-ci puissent se montrer plus productifs.

Et cette notion s'étend également aux interactions avec les clients : en tant que responsable des données de ses clients, l'entreprise d'aujourd'hui doit entretenir cette confiance de façon constante. Cette approche lui permettra de fidéliser ses consommateurs et de favoriser sa réussite, malgré le fait que les usurpateurs aient redoublé d'efforts pendant la pandémie. Dans ce contexte, la confiance passe d'abord par la sécurité – et l'identité en est le pilier. En d'autres termes, les marques numériques doivent fournir à leurs clients les outils nécessaires à une authentification transparente et sécurisée.

[1] IDC Perspective, 2020, Future of Trust: Defining Trust, April 2020, #US46185920

Récapitulatif de nos principales recommandations :

Les dirigeants et responsables informatiques doivent faire preuve de transparence avec les employés en situation de télétravail au sujet des mesures et politiques de cybersécurité mises en œuvre, et ce afin de gagner la confiance et d'emporter l'adhésion du personnel.

L'adoption de nouveaux outils de sécurité (comme l'authentification multifactorielle et la biométrie afin d'éliminer les mots de passe) est essentielle pour se protéger de l'usurpation des identités des consommateurs et sécuriser les accès à distance des professionnels.

Il est nécessaire de proposer davantage de formations en interne sur le phishing et les meilleures pratiques de sécurité, afin de limiter les risques liés au télétravail.

Maintenez votre stratégie de sécurité à jour afin de vous assurer qu'elle tienne compte de l'évolution des menaces, des réglementations relatives aux risques et des attitudes dignes de confiance (ou non).

Démontrez l'efficacité de vos mesures de sécurité à vos employés en télétravail, afin qu'ils se sentent protégés aussi bien à domicile qu'au bureau.

Les organismes gouvernementaux et services numériques doivent continuer de donner la priorité aux mesures de cybersécurité et de confidentialité afin de protéger les données des citoyens pendant la pandémie et dans le contexte actuel.

L'éthique relative au traitement des données est un paramètre important pour les clients. Les entreprises doivent donc s'assurer de respecter les recommandations visant à éviter l'utilisation abusive de ces informations et à réduire les risques de fuites de données.

Veillez à ce que votre organisation réponde aux nouvelles attentes des jeunes consommateurs en matière de sécurité et de confidentialité, afin de fidéliser un groupe démographique aussi important sur le plan économique.

«

La confiance est une réaction instinctive, précieuse, bénéfique et à risques ; et comme beaucoup de nos impulsions, il est parfois difficile de comprendre sur quels critères elle se base. L'étude d'Okta nous aide à comprendre comment notre confiance dans le numérique s'est transformée face à la situation sans précédent que nous vivons et qui nous a poussé à tout remettre en cause.

Ces résultats prouvent que la confiance des personnes s'établit plus sur des actions que sur des mots. Ce qui est une bonne chose, car placer la sécurité comme facilitateur est essentielle à la résilience et au succès des entreprises. Les résultats mettent également en évidence l'importance de la confiance dans la culture de la sécurité, c'est-à-dire cette nécessité pour les entreprises d'être plus transparentes avec les employés, les clients et les médias. A l'avenir, les dirigeants ne peuvent pas ignorer cette notion de confiance sinon ils passeront à côté de quelque chose.

Dr Jessica Barker, Cyber.UK

Partie 5

Sécuriser l'entreprise du futur grâce à Okta

L'identité est au cœur même des principes de confiance et de sécurité des organisations. Grâce à Okta Identity Cloud, les dirigeants d'entreprises du monde entier peuvent concevoir les meilleures expériences numériques pour leurs employés et leurs clients.

Sécurisez vos employés (où qu'ils se trouvent) grâce aux **solutions Okta de gestion des identités des employés**. Bénéficiez des outils nécessaires pour sécuriser et automatiser vos migrations vers le cloud, et profitez d'une prise en charge complète de vos environnements hybrides tout au long du parcours.

Utilisez les **solutions Okta de gestion des identités des clients** pour concevoir des expériences clients sécurisées et transparentes appréciées par vos développeurs et vos clients.

À propos d'Okta

Okta est le leader indépendant des services d'identification et de gestion d'accès pour les entreprises. Okta Identity Cloud permet aux organisations de proposer les technologies pertinentes aux individus adéquats, et au moment opportun. Grâce à plus de 6 500 intégrations préexistantes avec des applications et des fournisseurs de services logiciels, les clients d'Okta peuvent utiliser les technologies dont elles ont besoin pour mener à bien leurs activités, et ce de façon simple et sécurisée. Plus de 9 400 organisations à travers le monde – dont Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile ou encore Twilio – font confiance à Okta pour protéger les identités de leurs personnel et clients.

Okta.com/fr

okta