KASPERSKY lab

LE DÉFICIT DE COMPÉTENCES EN CYBERSÉCURITÉ: UNE BOMBE À RETARDEMENT

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW

Un mot d'Eugène Kaspersky

« Nous vivons à une époque où les organisations publiques et privées sont confrontées à des menaces de sécurité de plus en plus sophistiquées. Entreprises, infrastructures nationales stratégiques ou encore institutions financières, elles s'engagent dans une bataille perdue d'avance si elles ne disposent pas des employés ayant les compétences nécessaires pour lutter contre les cybercriminels.

Les jeunes technophiles peuvent combler le déficit de compétences qui touche les employeurs cherchant à lutter contre les cybermenaces et les intrusions en masse dans nos vies publiques et privées.

Les préoccupations relatives à la pénurie de cybercompétences combinées à un profond désir de résoudre le problème ont poussé Kaspersky Lab à commander une étude pour mieux comprendre le problème. Nous voulions découvrir comment les jeunes envisagent la cybersécurité en tant que carrière, et les implications potentielles pour les entreprises et la société dans son ensemble si le déficit de compétences continue de se creuser.

Les résultats de ce rapport sont frappants. Ils suggèrent que les jeunes d'aujourd'hui ont de grandes compétences dans le domaine numérique. Ils s'intéressent aux cyberattaques de grande envergure ainsi qu'à la recherche de moyens pour rendre leurs compétences utiles.

Toutefois, l'étude indique également que le secteur de la cybersécurité ne parvient pas à capter l'attention de cette génération, ni à fournir un chemin clair pour que les jeunes trouvent du travail, perfectionnent leurs compétences et servent la société. Au lieu de cela, beaucoup sont tentés d'utiliser leurs compétences du « côté obscur » en s'impliquant dans l'élaboration de cybermenaces, plutôt que dans leur prévention.

De plus en plus nombreuses, les cyberattaques menées par des adolescents profitent d'une notoriété grandissante. C'est pourquoi nous devons faire davantage pour encourager les jeunes à embrasser une carrière dans la cybersécurité et utiliser leurs compétences à bon escient. Nous devons canaliser les intérêts de la nouvelle génération de la bonne manière – avant qu'il ne soit trop tard et que nous nous retrouvions avec une pénurie de compétences plus importante encore. »

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

PRINCIPALES CONCLUSIONS

Un quart (27%) ont envisagé une carrière dans la cybersécurité, un grand nombre (47%) considérant qu'il s'agirait d'un bon usage de leur talent. Cependant, d'autres admettent utiliser leurs compétences pour le plaisir (17%), pour se livrer à des activités secrètes (16%) et pour gagner de l'argent (11%)

27%

23% des jeunes de 18 ans savent que quelqu'un qu'ils connaissent entreprend des cyberactivités susceptibles d'être illégales (ex : piratage)

23%

Plus de la moitié (57%) des moins de 25 ans considèrent le piratage comme une compétence « impressionnante »

57%

Les trois quarts (73%) des entreprises ont convenu qu'il était difficile de trouver suffisamment de professionnels en sécurité informatique

73%

87% des entreprises pensent qu'il est important que les jeunes se joignent à la lutte contre le cybercrime

87%

Introduction

Les organisations se rendent compte que la question n'est pas de déterminer **si** une cyberattaque se produira, mais **quand**. Cela incite les cadres à porter un intérêt croissant sur ce qui est fait pour protéger leur organisation. En conséquence, le soutien au développement de la cybersécurité est désormais bien établi. Le problème est que le bassin de talents qualifiés en cybersécurité ne se développe pas en parallèle.

La demande mondiale d'experts en cybersécurité devrait dépasser l'offre d'un tiers avant la fin de la décennie. L'étude internationale sur le marché du travail de Frost et Sullivan prévoyant une pénurie de 1,5 million de professionnels en sécurité d'ici 2020, selon les tendances actuelles. Les priorités doivent être rapidement orientées de manière à combler ce déficit avant qu'il ne soit trop tard.

Le secteur fait-il ce qu'il faut pour encourager davantage de jeunes dans les carrières de cybersécurité ? Les employeurs doivent-ils faire davantage pour canaliser l'intérêt et le talent des jeunes dans le domaine ? Peut-être les établissements d'enseignement devraient-ils mieux préparer les étudiants avec des cybercompétences plus avancées ?

D'ici la fin de la décennie, le nombre d'experts en cybersécurité devrait être inférieur d'un tiers à la demande...

Pour le savoir, Kaspersky Lab a mené une étude auprès d'environ 12,000 consommateurs et professionnels de l'informatique aux États-Unis et en Europe (Royaume-Uni, Allemagne, France, Italie, Espagne et Pays-Bas). Nous souhaitions découvrir comment combler ce déficit de compétences croissant, et qui doit être responsable de le combler.

Les résultats montrent que le déficit de compétences doit être comblé par un effort combiné du secteur et de l'enseignement, si nous voulons rendre les jeunes enthousiastes à l'idée de se lancer dans une carrière dans la cybersécurité. Cette génération est plus proche de la technologie que toute autre auparavant. Si cette connaissance est mal canalisée, le danger est que les génies de l'informatique soient bientôt tentés de s'engager dans une voie criminelle. Les jeunes doivent être mieux informés des possibilités de carrière qui existent dans la cybersécurité et doivent être encouragés à développer leurs compétences pour le bien de la société. En combinant l'enseignement et l'apprentissage sur le terrain, nous devons encourager les jeunes et les tourner vers la profession avant que le déficit ne se creuse encore.

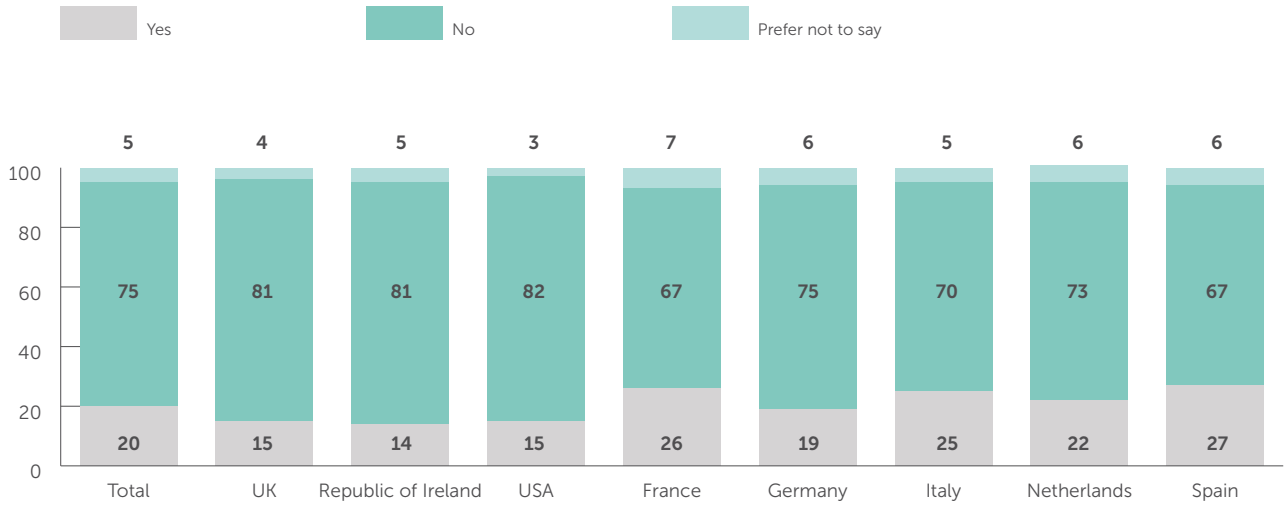
Les conclusions de l'étude

Les jeunes sont tentés d'exacerber la cybercriminalité, plutôt que de l'empêcher

Les jeunes adultes d'aujourd'hui sont hautement qualifiés tout en étant très impressionnables, alors qu'ils débutent un nouveau chapitre de leur vie – qu'il s'agisse de formation continue, quitter la maison ou démarrer un nouvel emploi. Nés dans un environnement numérique, ils y sont complètement immergés et sont habitués aux cyberattaques de grande envergure.

Nous avons constaté que 23% des jeunes de 18 ans savent qu'une personne qu'ils connaissent entreprend des cyberactivités susceptibles d'être illégales (ex : piratage). Ces activités sont plus fréquentes chez les jeunes universitaires (24%) et ceux qui viennent de quitter l'université et sont employés (23%). En comparaison, seuls 15% des jeunes en fin d'études sans emploi connaissent quelqu'un qui entreprend des cyberactivités susceptibles d'être illégales.

Avez-vous connaissance de possibles cyber-activités illégales (par exemple le piratage) auxquelles se livrait l'une de vos connaissances ?



Leur préoccupation ne dépasse que marginalement leur curiosité, et même leur respect, pour ces types de crimes. Un peu moins de la moitié (47%) des moins de 25 ans sont « impressionnés » lorsqu'ils entendent parler d'une entreprise piratée, et un tiers (33%) sont intéressés par la façon dont le piratage a été réalisé. Nous avons également constaté que la préoccupation augmente avec l'âge. 40% des 21–25 ans ont dit être préoccupés par l'étendue des dommages créés et par la façon dont l'entreprise réagira, comparativement à seulement 36% des jeunes âgés de 16 ans.

De façon alarmante, plus de la moitié (57%) des moins de 25 ans considère le piratage comme une compétence « impressionnante ». Nombreux sont ceux qui utiliseraient plutôt leurs compétences pour le plaisir (17%), les activités secrètes (16%), et le gain financier (11%).

Nombre d'entre eux sont déjà aptes à brouiller les frontières, avec un tiers des moins de 25 ans (31%) capables de cacher leur adresse IP, par exemple. Et avec seulement 50% qui affirment qu'ils seraient disposés à participer à la lutte contre la cybercriminalité de manière effective, il y a un manque clair d'engagement des jeunes dans la lutte contre la criminalité.

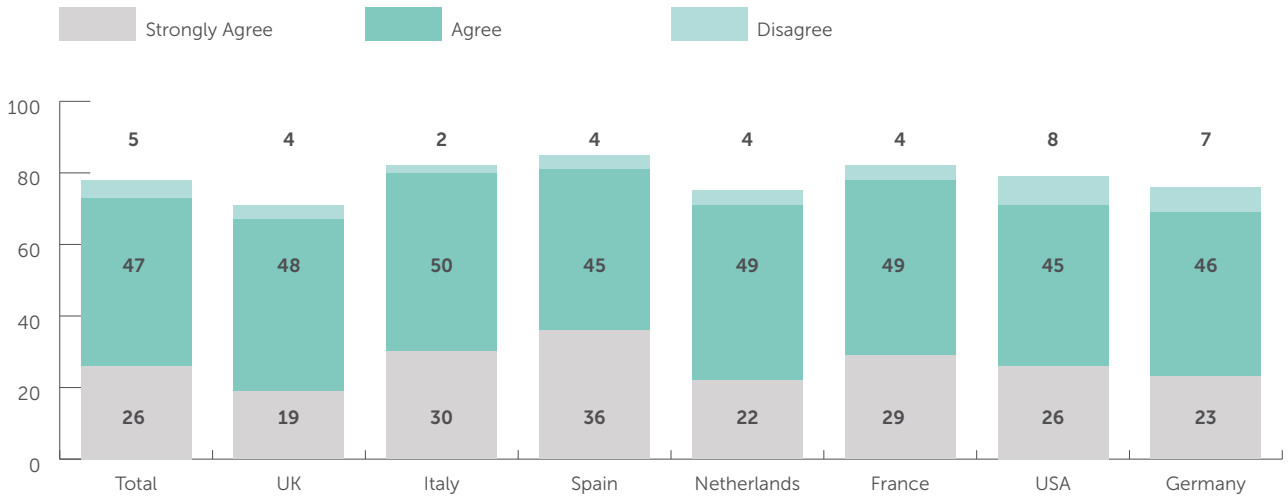
Les entreprises ont besoin de jeunes pour contribuer à la lutte contre la cybercriminalité

Avec un déficit toujours croissant des cybercompétences qui se profile, les jeunes passionnés d'informatique possèdent la clé pour occuper de nouvelles fonctions sur le front de la cybersécurité. Ce groupe possède les connaissances de base et la volonté d'apprendre, mais les employeurs ne parviennent pas à canaliser l'intérêt et le talent des jeunes vers ce domaine.

Un très grand nombre de professionnels du secteur (93%) reconnaissent que la profession doit évoluer en fonction du contexte actuel et futur, et 87% pensent qu'il est important que les jeunes se joignent à la lutte contre le cybercrime.

Le problème est que de nombreux employeurs n'ont pas de postes de cybersécurité pour les débutants ; la plupart la promeuvent de l'intérieur (72%), en fournissant une formation interne au besoin, et recrutent à l'extérieur (53%) des professionnels de la sécurité expérimentés.

Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : « Il est difficile de trouver suffisamment de professionnels en sécurité IT à recruter » ?

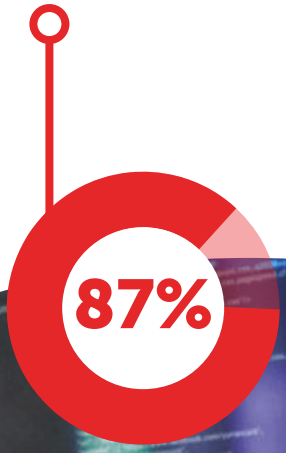


Il est important de reconnaître que les compétences en matière de sécurité se développent au fil du temps, tout comme pour d'autres professions dans l'informatique et ailleurs. On vous attribue une fonction qui est cohérente avec votre niveau de compétence, vous apprenez sur le tas et vous recevez une formation appropriée. Mais avec près de trois-quarts (73%) des entreprises qui éprouvent des difficultés à recruter des professionnels de l'informatique ayant les compétences appropriées, peut-être est-il temps de repenser les voies d'accès traditionnelles aux profession de la cybersécurité ?

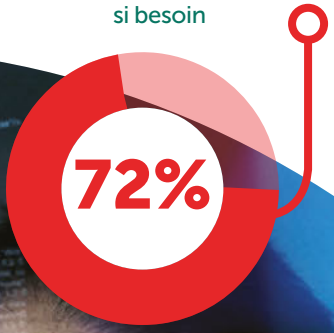
PRINCIPALES CONCLUSIONS

Une très large majorité de professionnels de l'industrie (93%) reconnaît la nécessité d'évoluer avec le paysage actuel et futur

87% pensent qu'il est important que les jeunes se joignent à la lutte contre le cybercrime



Le problème est que beaucoup d'employeurs n'ont aucun poste de débutant en cybersécurité à proposer ; la plupart privilégie les promotions internes (72%), offrant des formations internes si besoin

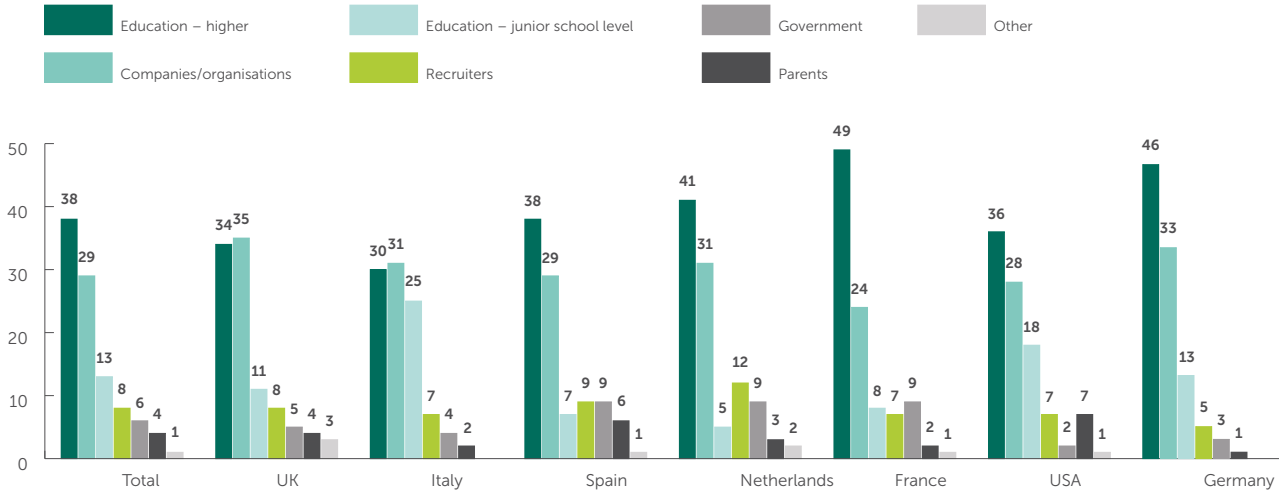


La responsabilité incombe-t-elle aux employeurs ou aux enseignants ?

La question de savoir qui est responsable d'impliquer la nouvelle génération de cyberdéfenseurs est importante, car l'ampleur du problème est claire. Nous avons besoin d'un plan qui se fonde sur l'intérêt manifeste, avant que cela ne conduise les esprits brillants et curieux à tourner le dos à la sécurité pour utiliser leurs compétences à des fins criminelles.

Selon le secteur de l'informatique, le système éducatif a un rôle clé à jouer pour encourager les jeunes talents dans la profession et les doter du niveau de compétences nécessaire. Notre recherche a révélé que près des deux tiers des professionnels de l'informatique (62%) ont estimé que les établissements d'enseignement doivent être les principaux responsables de la préparation des futures générations de professionnels de la cybersécurité. Le secteur a également un rôle clair dans la protection de son propre avenir, avec 27% de répondants estimant que la responsabilité première incombe à l'entreprise.

À qui incombe en priorité la responsabilité d'encourager les jeunes talents à rejoindre la profession ?



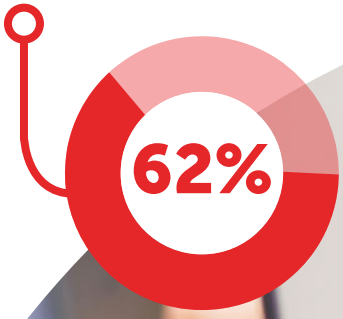
À la question de savoir si l'éducation ou l'entreprise est responsable d'encourager les jeunes à entrer dans le secteur, la recherche a révélé des différences régionales significatives. Les entreprises sont plus susceptibles d'être tenues responsables au Royaume-Uni, avec plus d'un tiers (35%) affirmant que les employeurs doivent en faire davantage pour aider les jeunes dans les fonctions de cybersécurité. En revanche, l'Italie (25%) et les États-Unis (18%) ont attaché une grande importance à l'éducation au niveau primaire, comparativement à une moyenne de 13%.

Pour ce qui est de veiller à ce que les jeunes aient les bonnes compétences en place, dans l'ensemble, une grande importance est accordée à l'enseignement supérieur (49%) ainsi que les entreprises et les organisations (27%). Mais, encore une fois, nous observons des différences régionales, avec par exemple de plus grandes attentes envers les employeurs aux Pays-Bas (40%).

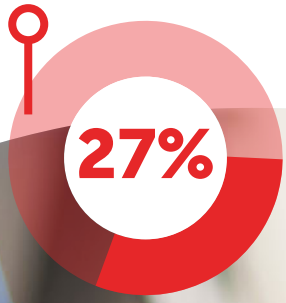
De toute évidence, les différences existent en raison des différents systèmes éducatifs et priorités gouvernementales mais, en vérité, nous avons besoin d'une approche commune entre les employeurs et l'enseignement pour fournir des compétences à une génération qui a soif de technologie et les développer.

PRINCIPALES CONCLUSIONS

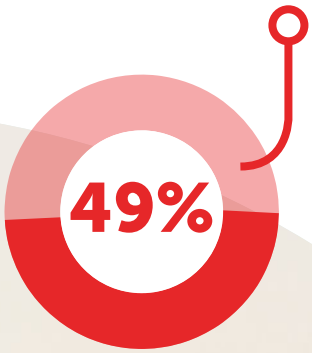
Notre recherche révèle que près de deux tiers des professionnels IT (62%) considèrent les établissement d'enseignement comme les premiers responsables de la préparation des futurs générations au métiers de la cybersécurité



Avec 27% des répondants qui jugent que cette responsabilité revient aux entreprise, l'industrie a également un rôle à jouer dans la pérennisation de son avenir



La responsabilité de former la jeune génération pour qu'elle dispose des connaissances adéquates est confiée avant tout à l'éducation supérieure (49%)



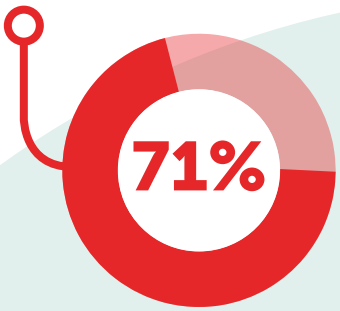
Assurer l'avenir du secteur de la sécurité

Il doit être fait davantage pour encourager et attirer les jeunes talents dans le secteur, car le déficit croissant de compétences en cybersécurité est une bombe à retardement. Nous avons constaté que près des trois quarts des jeunes (71%) ne sont pas informés des possibilités qui s'offrent à eux de poursuivre des études supérieures ou de réaliser des stages en sécurité informatique.

Bien que les entreprises soutiennent que les nouveaux arrivants ne possèdent pas les compétences pratiques nécessaires en matière de cybersécurité ou l'expérience, très peu proposent actuellement des postes pour débutants ou des stages qui peuvent permettre d'exploiter leur talent. En fait, seulement 45% disposent de postes pour débutants ou d'un programme d'études supérieures en place.

Trois sur dix (30%) admettent qu'elles ne disposent pas des ressources internes pour former les diplômés à une fonction de cybersécurité. Et de façon inquiétante, seul un cinquième (20%) des répondants estime qu'une équipe de cybersécurité dédiée aurait la responsabilité de la sécurité informatique d'ici cinq ans, avec moitié (50%) pensant qu'il incomberait à l'équipe informatique globale de lutter contre la cybercriminalité.

Nous avons constaté que près de trois quarts des jeunes (71%) ne sont pas informés des possibilités qui s'offrent à eux de poursuivre des études supérieures ou de réaliser des stages en sécurité informatique.



Quelle est la réponse ?

Du point de vue de Kaspersky Lab, ce rapport est le début d'un long voyage pour combler le déficit des cybercompétences, étant donné que la résolution d'un problème de cette ampleur nécessite des efforts coordonnés du secteur, de l'enseignement et du gouvernement.

Nous pensons qu'il doit être fait davantage au niveau des employeurs pour encourager les jeunes à se lancer dans des carrières de cybersécurité. Même parmi les professionnels de la sécurité informatique, 27% admettent que les organisations doivent faire davantage pour proposer des formations et des programmes pour les jeunes diplômés.

Les initiatives menées par l'industrie peuvent aider à promouvoir les carrières dans la cybersécurité. Les compétitions internationales pour les étudiants universitaires et jeunes professionnels encouragent par exemple les jeunes talents à utiliser leurs compétences en relevant divers défis de cybersécurité. Cela leur donne un avant-goût de la façon dont ils pourraient être utiles pour l'industrie et la société au sens large.

Travaillant en étroite collaboration avec les universités, notre secteur peut jouer un rôle dans le développement d'une pépinière de talents et veiller à ce que les enseignements théoriques et pratiques répondent aux attentes et aux besoins futurs. En consultant le matériel de cours, en assistant à des conférences, en promouvant la technologie et en collaborant dans la recherche, le secteur peut contribuer à susciter l'enthousiasme chez la prochaine génération de cyberdéfenseurs, à les impliquer, et surtout les éclairer et les éduquer. Proposer des emplois, des stages et des postes de diplômés aidera à cimenter la relation entre le secteur et l'enseignement, en garantissant que des compétences précieuses ne glissent pas à travers le filet au moment où nous en avons le plus besoin.

Les conclusions de ce rapport illustrent l'ampleur du défi auquel est confrontée l'industrie, mais soulignent également certains domaines où des progrès peuvent être accomplis. Nous devons adopter ces mesures pour désactiver la bombe à retardement de la cybersécurité avant qu'elle ne se déclenche.

1 Note de recherche : Kaspersky Lab a commissionné Arlington Research pour interroger un total de 2 120 professionals de l'informatique au Royaume-Uni, en Italie, en Espagne, aux Pays-Bas, en France, en Allemagne et aux Etats-Unis. D'autre part, Kaspersky Lab a commissionné Arlington Research pour interroger 11 531 jeunes consommateurs, âgés de 16 à 25 ans, au Royaume-Uni, en République d'Irlande, aux Etats-Unis, en France, en Allemagne, en Italie, aux Pays-Bas et en Espagne. Les deux études ont été complétées en juillet 2016.

KASPERSKY LAB

Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK

www.kaspersky.co.uk

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW