L'IA; menace pour lâ□□Ã©lection prÃ©sidentielle de 2024
Info
PostÃ© par : JerryG
PubliÃ©e le : 15/3/2024 13:00:00

Selon une nouvelle Ã©tude rÃ©alisÃ©e par Yubico et lâ□□organisation Defending Digital Campaigns, les deux partis (42â□□% de DÃ©mocrates et 49â□□% de RÃ©publicains) estiment que lâ□□IA aura un effet nÃ©gatif sur le rÃ©sultat du prochain scrutin.

Yubico, spÃ©cialiste des clÃ©s de sÃ©curitÃ© pour lâ□□authentification matÃ©rielle, et Defending Digital Campaigns (DDC), une organisation sans but lucratif et indÃ©pendante des partis qui a pour vocation de mettre des outils et des ressources de cybersÃ©curitÃ© gratuitement Ã la disposition des campagnes Ã©lectorales fÃ©dÃ©rales aux Ã□tats-Unis, rÃ©vÃ¨lent les conclusions de leur enquÃªte intitulÃ©e Â« Impact of cybersecurity and AI on the 2024 election season Â» (Impact de la cybersÃ©curitÃ© et de lâ□□IA sur la saison Ã©lectorale 2024).

RÃ©alisÃ©e par OnePoll, fournisseur majeur de solutions de communication spÃ©cialisÃ© dans les Ã©tudes de marchÃ© internationales, cette enquÃªte menÃ©e auprÃ¨s de 2 000 personnes inscrites sur les listes Ã©lectorales aux Ã□tats-Unis avait pour objectif de mieux comprendre la faÃ§on dont les Ã©lecteurs perÃ§oivent la cybersÃ©curitÃ© dans le contexte de lâ□□Ã©lection prÃ©sidentielle amÃ©ricaine qui aura lieu en novembre 2024, lâ□□impact de lâ□□intelligence artificielle (IA), et leurs prÃ©occupations quant Ã la cybersÃ©curitÃ© des campagnes politiques, indÃ©pendamment de leur appartenance Ã un parti.

Â«â□□Face Ã la progression soudaine de lâ□□intelligence artificielle et aux incertitudes quâ□□elle suscite, il nâ□□est pas surprenant de constater que plus de 78â□□% des personnes interrogÃ©es, Ã savoir 79 % de DÃ©mocrates et 80 % de RÃ©publicains, sâ□□inquiÃ¨tent de lâ□□utilisation de contenus gÃ©nÃ©rÃ©s par lâ□□IA pour usurper lâ□□identitÃ© dâ□□un candidat ou crÃ©er de faux contenus, explique David Treece, vice-prÃ©sident Solutions Architecture, Yubico. Plus rÃ©vÃ©lateur encore, 42â□□% de DÃ©mocrates et 49â□□% de RÃ©publicains estiment que lâ□□IA aura un effet nÃ©gatif sur le rÃ©sultat de la prochaine Ã©lection.â□□Â»

Outre la menace que reprÃ©sentent lâ□□IA et les deep fakes en diffusant de fausses informations, 85â□□% des personnes interrogÃ©es ne font guÃ¨re confiance aux responsables des campagnes politiques pour protÃ©ger efficacement leurs informations personnelles. Faute dâ□□Ã©lever la cybersÃ©curitÃ© au rang de prioritÃ©, les campagnes risquent par exemple de subir des failles, dâ□□exposer des donnÃ©es personnelles ou de subir des pertes financiÃ¨res, ce qui aurait des consÃ©quences nÃ©gatives sur lâ□□ensemble de la propagande Ã©lectorale.

Ainsi, 42â□□% des personnes ayant fait un don Ã une campagne ont dÃ©clarÃ© quâ□□elles nâ□□apporteraient probablement plus leur soutien financier en cas de piratage de la campagne, 30â□□% indiquant quâ□□une telle situation pÃ¨serait mÃªme sur la probabilitÃ© quâ□□un candidat reÃ§oive leur suffrage.

Â«â□□Les campagnes sont au cÅ□ur de notre dÃ©mocratie, et chaque campagne doit appliquer des mesures de protection Ã©lÃ©mentaires en matiÃ¨re de cybersÃ©curitÃ©. Lâ□□Ã©lection qui aura lieu en fin dâ□□annÃ©e prÃ©sente un risque Ã©levÃ© que des cyberattaques visent les candidats, les membres de leurs Ã©quipes et toute personne associÃ©e Ã leur campagne, ajoute Michael Kaiser, CEO de lâ□□organisation Defending Digital Campaigns.

La mise en place dâ□□une infrastructure de cybersÃ©curitÃ© adaptÃ©e nâ□□est pas une

possibilitÃ©, mais bel et bien une obligation pour tout responsable politique. Faute de quoi, les campagnes risquent non seulement de perdre des donnÃ©es prÃ©cieuses, mais Ã©galement des Ã©lecteurs.â□□Â»

Autres rÃ©sultats clÃ©s de cette enquÃªteâ□□

â□¢ 43â□□% des personnes interrogÃ©es ont la conviction que les contenus gÃ©nÃ©rÃ©s par lâ□□IA auront un impact nÃ©gatif sur le rÃ©sultat de lâ□□Ã©lection de 2024 ;
â□¢ 41 % des personnes ayant entendu un message enregistrÃ© avec une voix gÃ©nÃ©rÃ©e par lâ□□IA ont cru que la voix Ã©tait authentiquement humaine ;
â□¢ 52â□□% des personnes interrogÃ©es ont reÃ§u un email et/ou un texto provenant dâ□□une campagne et soupÃ§onnÃ© quâ□□il sâ□□agissait en rÃ©alitÃ© dâ□□une tentative de phishing ;
â□¢ Concernant la sÃ©curitÃ© des donnÃ©es, 85â□□% des personnes interrogÃ©es ne font guÃ¨re confiance aux responsables des campagnes politiques pour protÃ©ger efficacement les informations personnelles collectÃ©es ;
â□¢ Les Ã©lecteurs inscrits aimeraient que les campagnes et les candidatsâ□□:
Prennent des mesures Ã©vitant le piratage de leur site web (42â□□%),
Utilisent des mesures de sÃ©curitÃ© fortes telles que lâ□□authentification multi-facteurs (MFA) pour protÃ©ger leurs comptes (41â□□%),
Appliquent des rÃ¨gles, et forment leurs Ã©quipes et les principaux bÃ©nÃ©voles aux fondamentaux de la cybersÃ©curitÃ© dans le cadre de la campagne et afin dâ□□assurer la protection des informations personnelles (38â□□%) ;
â□¢ Plus dâ□□un quart des personnes interrogÃ©es (26â□□%) ont indiquÃ© ne pas avoir effectuÃ© de dons en faveur dâ□□une campagne Ã©lectorale, se dÃ©clarant prÃ©occupÃ©es par la sÃ©curitÃ© de la transaction ou la maniÃ¨re dont leurs informations personnelles sont traitÃ©es.

Â«â□□Dans la mesure oÃ¹ les campagnes reposent sur la confiance, des piratages potentiels tels que lâ□□envoi de courriels frauduleux ou de messages usurpant leur identitÃ© via leurs comptes de mÃ©dias sociaux dans le but dâ□□interagir directement avec les Ã©lecteurs potentiels, peuvent Ãªtre prÃ©judiciables aux responsables politiques, ajoute David Treece.

Il est primordial que les candidats prennent les mesures appropriÃ©es pour protÃ©ger leur campagne et, plus important encore, pour obtenir la confiance des Ã©lecteurs en adoptant des pratiques de cybersÃ©curitÃ© de nouvelle gÃ©nÃ©ration telles que lâ□□authentification rÃ©sistante au phishing. Lâ□□ajout aux comptes en ligne dâ□□une couche de protection matÃ©rialisÃ©e par une clÃ© de sÃ©curitÃ© physique telle quâ□□une YubiKey reprÃ©sente une dÃ©marche cruciale pour assurer la sÃ©curitÃ© des campagnes Ã©lectorales.Â»

Depuis 2020, Yubico a fait don de clÃ©s de sÃ©curitÃ© Ã lâ□□organisation Defending Digital Campaigns dans le cadre de son initiative philanthropique Secure it Forward. Plusieurs dizaines de milliers de YubiKeys ont ainsi Ã©tÃ© fournies Ã des journalistes, des militants des droits de lâ□□homme et des organisations qui ont pour vocation de veiller Ã la prÃ©servation de lâ□□intÃ©gritÃ© dÃ©mocratique, de promouvoir la diversitÃ© dans le domaine des hautes technologies et de protÃ©ger les droits humains.

Â« La collaboration reprÃ©sente lâ□□un des leviers les plus importants pour renforcer la cybersÃ©curitÃ©, prÃ©cise Michael Kaiser. Chez DDC, nous sommes extrÃªmement reconnaissants envers Yubico pour ce partenariat. La gÃ©nÃ©rositÃ© dont fait preuve Yubico nous permet de fournir gratuitement des clÃ©s de sÃ©curitÃ© aux responsables de campagnes Ã©lectorales et de leur permettre ainsi de bÃ©nÃ©ficier de protÃ©ger leurs comptes avec une efficacitÃ© maximale.

Les clÃ©s permettent Ã lâ□□utilisateur dâ□□un ordinateur de protÃ©ger les comptes cloud, sociaux et financiers de la campagne, mais Ã©galement les comptes personnels et les principales cibles des groupes malveillants.

Alors que la saison Ã©lectorale bat son plein, que peuvent faire les directeurs de campagne pour se protÃ©ger et gagner la confiance des Ã©lecteursâ□□? MÃªme si les cyberattaques gagnent en sophistication grÃ¢ce Ã des outils tels que lâ□□IA, il existe des moyens simples de limiter ces risques, par exemple en utilisant des mots de passe forts et uniques qui seront stockÃ©s dans un gestionnaire de mots de passe, ainsi quâ□□en activant lâ□□authentification multi-facteurs partout oÃ¹ cette option est disponible en utilisant une clÃ© de sÃ©curitÃ© physique comme en proposent Yubico et la DDC.

La DDC, une organisation sans but lucratif et indÃ©pendante des partis, sâ□□est engagÃ©e Ã fournir gratuitement des produits, des services, des sessions de formation et des informations de cybersÃ©curitÃ© aux campagnes et aux comitÃ©s politiques fÃ©dÃ©raux, ainsi quâ□□aux candidats en lice dans un nombre croissant dâ□□Ã□tats.

Elle sâ□□appuie sur un vaste rÃ©seau de partenaires et de ressources pour fournir aux campagnes Ã©lectorales les outils dont elles ont besoin pour prÃ©server leur cybersÃ©curitÃ©. En partenariat avec Yubico, la DDC fournit des YubiKeys gratuitement aux responsables politiques, quel que soit leur parti.

Pour consulter les ***rÃ©sultats de cette enquÃªte***,

Pour en savoir plus sur les programmes de lâ□□organisation ***Defending Digital Campaigns***,Â