Cyberespionnage : utilisation sécuritaire des webcams et des plateformes de vidéoconférence

Suivez ces six conseils pour choisir une plateforme de vidéoconférence sécuritaire et sécuriser votre webcam :

Méfiez-vous des services « gratuits »

Les entreprises qui offrent des services gratuits pourraient ne pas investir autant dans la sécurité. Faites vos recherches et envisagez d'opter pour une solution de vidéoconférence payante si les mesures de sécurité offertes sont plus solides. Au lieu d'utiliser la connexion gratuite et non sécurisée d'un point d'accès Wi-Fi, créez votre point d'accès personnel à l'aide de votre appareil mobile de l'entreprise.

Examinez votre espace de travail

Quels renseignements personnels ou confidentiels les objets qui se trouvent dans votre espace de travail pourraient-ils laisser transparaître? Une plateforme de vidéoconférence avec un arrière-plan virtuel ou un fond vert peut aider à cacher votre environnement personnel et les informations qui doivent rester confidentielles.

Sécurisez votre webcam

Pour éviter le cyberespionnage, éteignez votre webcam externe et utilisez-la uniquement lorsque vous en avez besoin. Pour une webcam interne, comme celles des ordinateurs portables, vous pouvez utiliser un cache-webcam ou placer une note autocollante (Post-it) sur la lentille de la caméra.

Restreignez l'accès aux réunions

Choisissez une plateforme dans laquelle il est difficile de cacher ou de modifier les informations permettant d'identifier les participants et demandez à chaque personne de s'annoncer au début de la réunion.

Misez sur un service de chiffrement de bout en bout

Le chiffrement de bout en bout est une mesure de sécurité supplémentaire qui rend les conférences et les communications plus difficiles à intercepter.

Installez des logiciels de sécurité

Assurez-vous que l'antivirus et l'anti-logiciel espion installés sur votre ordinateur sont bien à jour. Si vous voulez ajouter un autre niveau de protection pour votre webcam, vos ordinateurs et les autres appareils connectés à votre réseau résidentiel, il est conseillé de mettre en place un pare-feu ou de paramétrer votre routeur de manière à bloquer tout trafic entrant non désiré. Assurez-vous que votre réseau sans fil prévoit des paramètres de sécurité solides et un mot de passe fort pour empêcher des tiers d'accéder à votre réseau sans fil sans votre consentement.

ANCHOR
Solutions de risques

La Source : CyberScout