

# Lookout neutralise les attaques de phishing qui ciblent les cabinets d'avocats

Lookout Phishing and Content Protection protège les avocats contre les menaces mobiles

## Des défis de sécurité à l'échelle du secteur

Les cabinets d'avocats sont très dépendants des appareils mobiles, dans la mesure où ils leur permettent de répondre aux besoins de leurs clients de façon réactive. Ce qui signifie que de nombreuses informations dont ils sont tenus de respecter la confidentialité sont consultées en dehors du cabinet, et hors de la portée des outils de sécurité traditionnels. Le besoin de pouvoir travailler à tout moment et en tout lieu signifie que les appareils sont utilisés aussi bien dans un cadre personnel que dans un cadre professionnel, ce qui pose souvent un problème de sécurité et de confidentialité pour les avocats. Le fait de mélanger les appareils personnels et professionnels représente également un défi majeur pour les cabinets d'avocats, en particulier à l'heure où on stocke de plus en plus les données des clients sur des services Cloud.

## Étude de cas concrète concernant les cabinets d'avocats

Dans la mesure où ils utilisent des appareils mobiles, les avocats sont une cible privilégiée pour les attaques de phishing. Néanmoins, ils disposent généralement de systèmes de sécurité traditionnels. En réalité, 80 % des cabinets d'avocats ont indiqué avoir été la cible d'attaques de phishing en 2018. L'objectif de ces attaques est d'intercepter des identifiants d'entreprise sur le Cloud afin d'accéder à des informations client sensibles. C'est pourquoi les équipes chargées de l'informatique et de la sécurité doivent être en mesure de proposer des outils de sécurité capables d'identifier des liens de phishing sur les appareils mobiles, en particulier dans les e-mails personnels et professionnels, les messages et les applications de réseaux sociaux.



### Défis du secteur

1. Des appareils mobiles largement utilisés par tous les employés du cabinet.
2. Une protection des données personnelles sensibles des clients et des documents de leur dossier.
3. Un mélange accru d'applications professionnelles et personnelles qui augmente le risque d'attaques de phishing envoyées via des plateformes de messagerie et de réseaux sociaux.

## La fonctionnalité stratégique de Lookout

Lookout Phishing and Content Protection inspecte toutes les demandes d'URL, notamment les e-mails personnels et professionnels, les SMS, les applications de messagerie et les applications comportant des URL pour télécharger des plug-ins malveillants. Lookout bloque de façon dynamique les demandes d'URL pour accéder à des sites Web identifiés comme étant malveillants. Par exemple, si cette fonctionnalité est activée, Lookout peut empêcher un employé victime de phishing de saisir des identifiants de connexion dans la réplique malveillante d'une page de connexion Office 365. En outre, pour assurer la confidentialité de l'utilisateur, il suffit que Lookout signale l'existence d'un problème et le nombre de détections à la console MES. Les administrateurs ne peuvent pas afficher l'historique de navigation ou le trafic d'un appareil.

## Pourquoi choisir Lookout ?

La solution Lookout Mobile Endpoint Security avec accès conditionnel continu assure la sécurité et la conformité de tous les appareils grâce à un ensemble de données considérable, alimenté par plus de 170 millions d'appareils et l'analyse de plus de 70 millions d'applications mobiles. Lookout Security Cloud facilite le déploiement de Lookout et la mise en place de politiques de sécurité dans l'ensemble de l'organisation, tant pour les appareils gérés que pour les appareils non gérés. Les utilisateurs reçoivent en temps réel des alertes et des étapes à suivre pour corriger les problèmes concernant les applications malveillantes, les connexions au réseau et les anomalies du système. Ils bénéficient également d'une vérification dynamique de l'état de santé de l'appareil afin d'assurer un accès conditionnel continu aux applications et aux données sensibles d'entreprise.

<sup>1</sup>National Cyber Security Centre : <https://www.ncsc.gov.uk/report/the-cyber-threat-to-uk-legal-sector-2018-report>