Pourquoi les entreprises doivent-elles se protéger contre le phishing sur mobile ?

D'après Lookout, les utilisateurs de terminaux mobiles ont trois fois plus de risques d'être victimes d'attaques de phishing. En fait, 56 % des utilisateurs ont déjà reçu et cliqué sur une URL de phishing sur leur appareil mobile. Ces utilisateurs ont cliqué, en moyenne et en un an, sur six URL de phishing sur leur appareil mobile.

3x

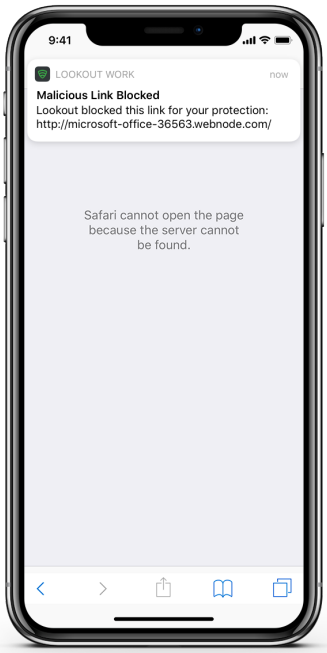
Les utilisateurs de terminaux mobiles en entreprise ont trois fois plus de risques de cliquer sur un lien de phishing sur un petit écran que sur un ordinateur de bureau.

Or, si un attaquant parvient à inciter un utilisateur à fournir ses identifiants, il pourra alors accéder aux systèmes de l'entreprise et parcourir vos infrastructures et données sans être détecté.

Quelle protection offre Lookout contre le phishing ?

La protection des contenus et contre le phishing de Lookout, fonctionnalité complète de Lookout Mobile Endpoint Security, a été conçue pour protéger les entreprises contre les attaques de phishing, quel que soit le canal, y compris les e-mails (professionnels et personnels), les SMS, les applications de messagerie et les URL intégrées dans des applications.

Lookout inspecte les requêtes du terminal qu'un navigateur ou une application cherche à se connecter à Internet. Là où cette approche se démarque, c'est qu'elle ne nécessite aucune inspection du contenu des messages et n'enfreint donc pas la vie privée des utilisateurs finaux. Lookout compare l'URL à laquelle l'utilisateur cherche à accéder à toutes les URL malveillantes connues et identifiées par Lookout Security Cloud. Si elle est malveillante, Lookout le signale à l'utilisateur final avant la fin de la connexion. Ce système d'alerte en temps réel évite toute exposition à des contenus risqués, comme des applications ou des sites Web malveillants, dont les vulnérabilités sont connues.



La console de Lookout permet aux administrateurs de bloquer les utilisateurs cherchant à se connecter sur leur appareil mobile à des URL malveillantes connues hébergées sur des sites Web à risque et susceptibles de dérober leurs identifiants.

Ces URL malveillantes peuvent être des publicités frauduleuses, des botnets, des centres de commande et de contrôle, des liens compromis et redirigeant vers des logiciels malveillants, des call home de logiciels malveillants, des points de distribution de logiciels malveillants, du phishing/de la fraude, des URL spam et des logiciels espions.

Par défaut, cette fonctionnalité n'est pas activée sur Lookout Mobile Endpoint Security. Un administrateur doit activer la protection des contenus et contre le phishing dans la console et l'utilisateur final doit donner les autorisations nécessaires sur l'appareil à protéger.

Avant le blocage de sites Web à risque, les administrateurs peuvent également choisir d'en informer les utilisateurs. Si la protection des contenus et contre le phishing est désactivée sur l'appareil d'un utilisateur, les administrateurs pourront marquer l'appareil comme non conforme jusqu'à la réactivation de la protection.

Pourquoi choisir Lookout ?

Protégez vos terminaux mobiles en ajoutant une ligne de protection puissante contre le phishing, qui couvre les e-mails personnels, les SMS, les plates-formes de messagerie et les applications.

Accélérez votre transformation numérique en utilisant en toute confiance des terminaux mobiles au travail et en les protégeant contre les contenus malveillants, que les employés soient connectés au réseau protégé de leur entreprise ou non.

Bénéficiez d'une protection complète à grande échelle, couvrant tout le spectre des risques mobiles, y compris les menaces web, l'un des vecteurs mobiles que les attaquants utilisent le plus souvent pour exfiltrer des données d'entreprises.

Ce qui rend Lookout différent

- Grâce à notre présence mondiale et à l'importance que nous accordons au mobile, Lookout a réuni l'un des ensembles de données sur la sécurité mobile les plus importants au monde. Lookout a ainsi collecté les données de sécurité de plus de 170 millions d'appareils à travers le monde et de plus de 70 millions d'applications, avec jusqu'à 90 000 nouvelles applications ajoutées quotidiennement.
- Ce réseau de capteurs mondial intègre la notion de prévisibilité à notre plate-forme en laissant l'intelligence artificielle identifier les modèles complexes synonymes de risque, modèles qui autrement échapperaient aux analystes humains.
- La mobilité a fait entrer l'informatique dans une nouvelle ère et nécessite une nouvelle solution de sécurité conçue exclusivement pour ses besoins. Lookout sécurise les appareils mobiles depuis 2007 et possède une solide expérience en la matière.

En fournissant aux équipes informatiques et de sécurité la visibilité dont elles ont besoin, Lookout permet à votre entreprise d'intégrer la mobilité à son écosystème en toute sécurité et sans sacrifier la productivité. Pour découvrir dès aujourd'hui comment sécuriser votre parc mobile, visitez notre site à l'adresse suivante : lookout.com/fr.