## Darum müssen sich Unternehmen vor Phishing-Angriffen auf Mobilgeräten schützen

Statistisch gesehen fallen Nutzer von Mobilgeräten dreimal häufiger auf Phishing-Betrug herein, als auf PCs oder Laptops. Laut Lookout haben 56 % aller Anwender bereits Phishing-URLs über ihr Mobilgerät aufgerufen. Im Jahresdurchschnitt blockierte Lookout sechs Phishing-URLs auf diesen Geräten.

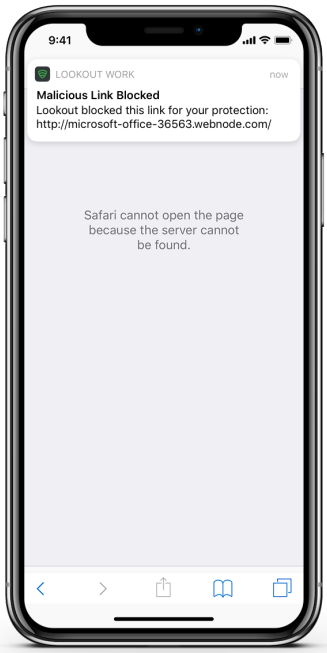
**3x** Unternehmensanwender fallen dreimal häufiger auf Phishing-Betrug herein, wenn sie ein Mobilgerät anstelle eines Desktopcomputers nutzen.

Wenn es einem Angreifer gelingt, einen Anwender dazu zu verleiten, Firmenzugangsdaten preiszugeben, erhält er Zugriff auf Unternehmenssysteme, sodass er sich ungehindert durch die Infrastruktur bewegen und Daten ausspionieren kann.

## So schützt Lookout vor Phishing-Angriffen

Der Phishing- und Content-Schutz von Lookout ist eine umfassende Funktionalität von Lookout Mobile Endpoint Security, die Unternehmen vor Phishing-Angriffen über sämtliche Kanäle wie E-Mail (geschäftlich und privat), SMS, Messaging-Apps und in Apps eingebettete Browser und URLs schützt.

Dafür überwacht Lookout sämtliche ausgehenden Verbindungen des Mobilgeräts und aller installierten Apps auf Netzwerkebene. Da dabei der Inhalt von Nachrichten nicht überprüft wird, bleibt die Privatsphäre des Endnutzers gewahrt. Dadurch unterscheidet sich unser Ansatz von herkömmlichen Lösungen. Lookout vergleicht die URL, die geöffnet werden soll, mit bekannten präparierten URLs in der Lookout Security Cloud und warnt den Anwender im Ernstfall, bevor eine Verbindung hergestellt wird. Diese Echtzeitwarnungen verhindern, dass der Anwender gefährliche Webseiten öffnet oder sich Malware installiert.




Über die Lookout-Konsole können Administratoren Verbindungen zu bekannten schädlichen URLs blockieren, die über präparierte Websites gehostet werden und möglicherweise versuchen, Zugangsdaten zu erlangen.

Als schädliche URLs gelten betrügerische Anzeigen, Botnets, Command and Control Center (C&C), Links zu Malware, Malware Call Home, Malware-Verteilungspunkte, Phishing/Betrug, Spam-URLs und Spyware.

In Lookout Mobile Endpoint Security ist diese Funktionalität standardmäßig deaktiviert. Ein Administrator muss den Phishing- und Content-Schutz erst in der Konsole aktivieren und der Anwender muss auf dem Gerät die nötigen Berechtigungen erteilen.

Administratoren haben auch die Möglichkeit, Anwender vor gefährlichen Websites zu warnen, bevor diese sie öffnen. Und wenn der Phishing- und Content-Schutz auf einem Gerät deaktiviert ist, können diese Geräte automatisch als nicht konform markiert werden, bis der Schutz wieder aktiviert wird.

## Warum Lookout

Mit Lookout dehnen Sie Ihren Phishing-Schutz auf Mobilgeräte aus, der dann private E-Mails, SMS, Messaging-Plattformen und Apps abdeckt.

So unterstützen Sie den digitalen Wandel, denn damit steht der Nutzung von Mobilgeräten für die Arbeit nichts mehr im Wege. Ihre Daten und Systeme sind vor schädlichen Inhalten geschützt, unabhängig davon, ob sich der Mitarbeiter innerhalb des geschützten Unternehmensnetzwerks befindet oder nicht.

Lookout bietet umfassenden Schutz vor allen Facetten mobiler Risiken, einschließlich des Web- und Content-Bedrohungsvektors, der von Angreifern am häufigsten genutzt wird, um Unternehmensdaten über Mobilgeräte auszuspähen.

### Lookout – der große Unterschied

- Dank unserer globalen Ausrichtung und unserer Konzentration auf Mobilgeräte verfügt Lookout über einen der weltweit größten Datensätze zur mobilen Sicherheit. Lookout hat Sicherheitsdaten von über 170 Millionen Geräten weltweit sowie über 70 Millionen Apps erfasst. Täglich kommen bis zu 90.000 neue Apps hinzu.
- Dank dieses globalen Sensorennetzwerks kann unsere Plattform Bedrohungen im Voraus erkennen. Wir setzen dafür maschinelle Intelligenz ein, um komplexe Muster zu identifizieren, die auf Risiken hindeuten. Diese Muster wären für menschliche Analysten nicht erkennbar.
- Die Mobilität hat eine neue Ära der Datenverarbeitung eingeläutet. Benötigt wird eine neue Generation von Sicherheitslösungen, die speziell für diese Plattform entwickelt wurden. Lookout spezialisiert sich bereits seit 2007 auf mobile Sicherheit und verfügt über das gebotene Expertenwissen in diesem Bereich.

Mithilfe von Lookout können Ihre Mitarbeiter sicher mobil unterwegs sein, und zwar ohne Einbußen bei der Produktivität, denn Lookout versorgt die IT- und Sicherheitsteams mit der erforderlichen Transparenz. Mehr darüber, wie Sie Ihre Mobilgeräteflotte noch heute besser absichern können, erfahren Sie auf lookout.com/de.