Black Friday: Deals, Deals, Deals – oder?

Sophos nennt 10 grobe Fehler, die Hacker jubeln lassen

Der Black Friday steht vor der Tür – ein Shopping-Event für die Konsumenten, ein Fest für die Cybergangster. Möchten Sie denen auch mal eine Freude machen? Dann befolgen Sie einfach eine oder – ach was! – am besten gleich alle unserer zehn schwarzen Regeln.

Aber im Ernst: nehmen Sie sich unsere kleine Aufzählung ruhig insofern zu Herzen, als dass Sie sich ganz ehrlich fragen, welchen dieser Fehler Sie vielleicht wirklich noch begehen.

1. **Verwenden Sie ein Passwort, das leicht zu merken ist.**
   Oder zu erraten. Vielleicht etwas Schlichtes wie '123456'. So etwas Einfaches hat vermutlich keiner und es kommt auch niemand drauf. Außer Cybergangstern natürlich. Die knacken so etwas innerhalb von Sekunden.

2. **Verwenden Sie immer dasselbe Passwort.**
   Egal ob Facebook, Google, Banking-Account, Shopping-Kanal – machen Sie es sich und den Hackern leicht und schützen Sie alles mit ein und demselben Passwort. Der Hacker muss so nur ein einziges Mal Ihr Passwort knacken und hat Zugang zu allen Accounts.

3. **Legen Sie sich unbedingt ein Dokument mit allen Passwörtern auf Ihrem Smartphone oder im E-Mail-Account an.**
   Wer mehrere Passwörter verwendet, muss diese schließlich irgendwo vermerken. Freut auch den Hacker, der leichter Zugang zu ihrem Ordner hat, als Sie es sich vielleicht vorstellen. Sie könnten natürlich auch eine Passwort-Management Software verwenden, die Ihre Passwörter automatisch und sicher verwaltet. Aber das wäre wirklich zu gemein für den Hacker.

4. **Ignorieren Sie um Himmels Willen die ständigen Aufforderungen zum Software-Update auf Laptop, PC, iPad und Smartphone.**
   Das hat sich die Industrie nur ausgedacht, um Sie wahnsinnig zu machen. Mit Datensicherheit hat das rein gar nichts zu tun. Und ob diese Updates wirklich Lücken schließen, durch die Kriminelle eindringen können, weiß man ja gar nicht.

5. **Öffnen Sie ruhig Links oder Anhänge von Ihnen völlig unbekannten Absendern.**
   Schließlich müssen Sie ja wissen, was es mit der Zahlungsanweisung, der Kontaktaufnahme, der Erbschaft etc. auf sich hat. Sowohl die Anhänge als auch Links in solchen Mails sind bestimmt völlig unbedenklich, wer wird denn immer so misstrauisch sein? Und wenn Ihre eigene Bank Ihnen schreibt und Sie auffordert Ihr Passwort zu ändern, dann ist das sehr freundlich und offenbar ein neuer Service – in den letzten 20 Jahren hat sie das schließlich bisher noch nie getan.

6. **Beantworten Sie freundlich alle E-Mails, die mit „Lieber Kunde" beginnen** und Sie darauf hinweisen, dass man auf Ihrem Account unübliche oder verdächtige Aktivitäten festgestellt hat. Wie nett, Sie darauf hinzuweisen. Dass hiermit womöglich versucht wird, Ihre Zugangsdaten zu stehlen um dann Ihren Account zu übernehmen und für sonstwas zu missbrauchen gehört bestimmt ins

Reich der Verschwörungstheorien.

7. **Nutzen Sie die praktische Erinnerungs-Funktion, wenn Sie sich auf einer Seite einloggen.** Immerhin haben die Programmierer sich etwas dabei gedacht, als sie diese Funktion eingebaut haben. Warum also nicht benutzen? Besonders beim Online-Banking ist es enorm praktisch, das Sicherheitspasswort nicht andauernd eingeben zu müssen. Und es merkt ja niemand. Ausser Ihnen ist ja niemand an Ihrem Computer, stimmts?

8. **Nutzen Sie die unglaublich guten Angebote, machen Sie tolle Schnäppchen**. Darum geht es schließlich am Black Friday. Markensonnenbrillen mit 70 Prozent Rabatt? Ein kostenloses iPhone als Begrüßungsgeschenk? Wieso sollte man da denn misstrauisch werden? Vielleicht haben Sie ja einfach mal Glück? Dafür ist doch Cyber-Friday: für 1A Deals und tolle Chancen – auch für Kriminelle.

9. **Verbinden Sie sich sorglos mit fremden WLAN-Netzen und shoppen Sie auch von unterwegs**. Man will ja nichts verpassen. Fremde Netze sind bestimmt vernünftig abgesichert. Wäre dem nicht so, könnte ja Ihr Datenverkehr von Kriminellen mitgelesen und verwendet werden.

10. **Und Kontobewegungen müssen Sie nun wirklich nicht überprüfen.** Schließlich haben wir alle genug zu tun. Es werden schon keine Transaktionen ohne Ihr Wissen vorgenommen – wie denn auch? Sie haben ja Ihre Zugangsdaten niemandem mitgeteilt.

Wie gesagt, tasächlich ***nicht*** nachmachen und lieber ehrlich prüfen, ob Sie einen dieser Fehler vielleicht doch noch begehen. Passen Sie auf sich auf. Wir wünschen einen sicheren Cyber-Friday und tolle echte (!) Schnäppchen.

23. November 2016

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de