

## Tatort Facebook, Spurensuche auf Twitter – warum F-Secure zu separaten Passwörtern rät

**München, 17. September 2009 – Weltweit bekannte soziale Media-Netzwerke wie Facebook und Twitter sind in das Visier krimineller Online-Angriffe wie Phishing und Spammen geraten. Denn Attacken auf einen einzelnen User haben in der Regel Auswirkungen auf das gesamte Netzwerk, zudem bieten solche Communities Zugang zu vertraulichen Informationen. Sicherheitsexperte F-Secure rät den Usern zu einfachen Präventivmaßnahmen.**

Derzeit versuchen global agierende Hacker vermehrt, sich mit gefälschten, aber wirkungsvollen E-Mails Zugangsdaten von Facebook-Nutzern zu verschaffen. Erst kürzlich kam es zu einem großen Angriff, der Facebook und Twitter für mehrere Stunden lahm legte und kurzfristig sogar zum Zusammenbruch der Seiten führte. Mikko Hyppönen, Chief Research Officer bei F-Secure: „Auch wenn solche Attacken nur an einzelne Personen gerichtet sind, haben sie Auswirkungen auf die gesamte Community eines Social Networks.“

### **Schwarze Schafe unter 250 Mio. Usern**

Im internationalen Vergleich sind die Deutschen mit 37% die Schlusslichter der Aktivitätsskala in sozialen Netzwerken wie Facebook, Twitter und Xing. Mit 88% Aktivitätsindex stehen die Polen an der Spitze, gefolgt von den Italienern (69%), Finnen (66%), Engländern (61%), Schweden (54%) und Amerikanern (43%). Das zeigt eine internationale Studie von F-Secure vom August 2009. Die Kommunikation über Netzwerke wie Facebook basieren auf der persönlichen Verbindung der User. Dabei ist ein hoher Grad an Vertrauen im Spiel. Eine persönliche Nachricht von einem Freund an der eigenen Pinnwand hat einen ganz anderen Stellenwert, als eine anonyme E-Mail oder gar Spam zu bekommen. Genau dieses vertraute Umfeld und die hohe Anzahl von mittlerweile weltweit 250 Millionen Usern macht Facebook zu einem attraktiven Ziel für Kriminelle. Phishing und finanzieller Betrug funktionieren nur mit einer suggerierten persönlichen Nachricht, die das Vertrauen der Zielperson wecken soll. Fällt der User darauf hinein, gelangt der Kriminellen an vertrauliche Informationen oder gar finanzielle Begünstigungen.

Dieses Jahr erreichten schon viele Facebook-User betrügerische Nachrichten von vermeintlichen „Freunden“, die nach finanzieller Hilfe fragten. Facebook-User sollten solche Anfragen immer mit höchster Vorsicht genießen und einen kritischen Identitäts-Check machen, bevor sie Geld versenden - auch wenn die Nachricht von einem Familienmitglied oder einer anderen Person des Vertrauens kommt.

### **Das Passwort ist des Users Identität**

Auch besonders kritische User können ausgetrickst werden, wenn sie leichtsinnig mit der Passwortvergabe umgehen. Sean Sullivan, Sicherheitsberater bei F-Secure: „Unsichere Passwörter sind nach wie vor der einfachste Weg für Kriminelle, sich in die Profile von sozialen Netzwerken einzuhacken. Ziel ist es, an die Kontaktdaten und Telefonnummern zu kommen, die sich an Spammer verkaufen lassen oder bei zielgerichteten Angriffen gewinnbringend einsetzen lassen.“

Der Schaden ist umso größer, wenn das Passwort des Facebook-Profiles mit dem des privaten E-Mail-Accounts identisch ist. Denn dann hat der Kriminelle die Möglichkeit, diese Online-Passwörter zu verändern, sich Zugang zu Bankdaten zu verschaffen und

### Kontakte für die Presse:

Sandra Proske  
F-Secure GmbH  
Zielstattstraße 44  
81379 München

Tel.: +49 89 787 467-22  
Fax: +49 89 787 467-99  
[sandra.proske@f-secure.com](mailto:sandra.proske@f-secure.com)  
[www.f-secure.de](http://www.f-secure.de)

Berk Kutsal / Jürgen Rast  
Trademark PR GmbH  
Goethestraße 66  
80336 München

Tel.: +49 89 444.467-461  
Fax: +49 89 444.467-479  
[f-secure@trademarkpr.eu](mailto:f-secure@trademarkpr.eu)  
[www.trademarkpr.eu](http://www.trademarkpr.eu)

schneller Lücken in den Sicherheitsvorkehrungen zu finden. Nicht selten können vertrauliche Informationen wie der zweite Vorname, die persönliche Anschrift oder der Name des Haustiers direkt bei Facebook eingesehen werden.

„Da der Facebook-Username die Mailadresse als Bestandteil hat, ist es von großer Wichtigkeit, dass sich die Passwörter für Facebook und den privaten E-Mail-Account unterscheiden. Zudem ist es sicherer, wenn man mehrere E-Mail-Adressen nutzt, beispielsweise eine für die Arbeit, eine für private Korrespondenz und eine eigene für soziale Netzwerke“, so Sullivan.

Der Blick auf die internationalen Umfrageergebnisse von F-Secure zeigt, dass die Deutschen in Sachen Passwortsicherheit weit vorne liegen. 82% nutzen verschiedene Passwörter für soziale Netzwerke und den eigenen E-Mail-Account. Nur die Finnen toppen das mit 84%. Polen zieht mit Deutschland gleich (82%), dicht gefolgt von den Schweden (81%), Engländern (75%), Amerikanern (74%) und Italienern (74%).

„Es gibt aber auch einen positiven Sicherheitsaspekt der sozialen Netzwerke. Anders als die klassischen E-Mail-Betrügereien wie Kettenbriefe, die jahrelang laufen, trägt die Erfahrung der Facebook-User dazu bei, dass sich die Nachricht über eine Sicherheitsbedrohung sehr schnell verbreitet. Eine Community agiert und reagiert sehr schnell, verbreitet unter den Mitgliedern hilfreiche Sicherheitstipps und Präventivmaßnahmen und gibt darüber hinaus Anregungen für die Schadensbehebung“, so Sullivan.

F-Secure rät für einen sicheren Umgang mit sozialen Netzwerken:

1. Immer unterschiedliche Passwörter für Netzwerke und E-Mail-Accounts benutzen.
2. Wenn man auf eine Sicherheitsbedrohung im sozialen Netzwerk aufmerksam wird, sofort eine Nachricht an die Pinnwand schreiben, damit die Community Präventivmaßnahmen ergreifen kann.
3. Freunde bedacht auswählen und wenn möglich einen „Sicherheits-Guru“ unter den Freunden haben.
4. Facebook-Fan von F-Secure werden, um stets die aktuellsten Sicherheitshinweise und Informationen zu bekommen.
5. Eine Internet-Security-Software installieren und regelmäßig updaten oder das automatische Update aktivieren (beispielsweise Internet Security 2010 von F-Secure).

## Über F-Secure

Innovation, Zuverlässigkeit und Schnelligkeit – diese drei Qualitäten haben F-Secure seit der Gründung 1988 zu einem der führenden IT-Sicherheitsanbieter weltweit gemacht. Heute vertrauen sowohl Millionen Privatanwender als auch Unternehmen auf die mehrfach ausgezeichneten Lösungen von F-Secure. Der effektive Echtzeitschutz arbeitet zuverlässig und unbemerkt im Hintergrund und macht das vernetzte Leben von Computer- und Smartphone-Nutzern sicher und einfach.

Die Lösungen von F-Secure sind als Service-Abonnement über mehr als 200 Internet Service Provider und Mobilfunkbetreiber weltweit zu beziehen. Die umfangreichen Partnerschaften machen F-Secure zum Marktführer in diesem Bereich. Seit 1999 ist das Unternehmen an der Börse in Helsinki notiert (NASDAQ OMX Helsinki Ltd.). Seitdem wächst F-Secure schneller als viele andere börsennotierte Mitbewerber.

Ständig aktuelle Informationen über die neuesten Viren finden sich im Weblog des „F-Secure Antivirus Research Teams“ unter der Internetadresse [www.f-secure.com/weblog](http://www.f-secure.com/weblog).