Wichtigste Tipps zur Bekämpfung von Spam

Unter Spam wird eine massenweise per E-Mail und Instant Messaging verteilte direkte Werbung verstanden; sie bezieht sich am häufigsten auf „Schnell reich werden“-Angebote, fragwüdige Produkte, betrügerische Angebote oder pseudo-legale Dienste. Durch Spam wird der Verbraucher getäuscht, das Konsumentenvertrauen untergraben und legitimen Internethändlern, die ethische Praktiken anwenden, geschadet. Spam kann vom Sender mühelos verteilt werden, stellt aber eine erhebliche Belastung für die Empfänger dar. Außerdem kann Spam sehr gefährlich sein, da Internetkriminelle über Spam betrügerische Phishing-E-Mails senden. Die Anzahl der Phishing- und Pharming-Programme ist in die Höhe geschnellt; Kriminelle stehlen Identitäten und kidnappen Systeme mithilfe von komplexen Angriffen, bei denen die Anwender durch Spam auf Websites geleitet werden, die mit Trojanern, Spyware und Angriffscodes gespickt sind.

Weblogs, allgemein als Blogs bezeichnet, verzeichnen eine steile Zunahme an Spam. Unter „Splog“ wird ein Angriff von Junk-Mitteilungen verstanden, die wie tatsächliche Nutzerkommentare aussehen, jedoch Werbelinks zu Websites enthalten.

Für eine sichere Nutzung ihres Computers und des Internets müssen Verbraucher ihre Dateien, ihre Identität und persönlich Daten absichern und die gesamte Online-Nutzung für sich selbst und ihre Familie schützen. Durch die Befolgung der in diesem Artikel aufgeführten Tipps können Anwender die mit Spam verbundenen Risiken besser reduzieren und sich vor Hackern, Spammern und Phishern schützen.

Wie gelangen Spammer an meine Adresse?

Spammer kaufen Listen von Maklern, die E-Mail-Adressen aus Newsgroups, Chatrooms, Websites, Social Network-Seiten wie MySpace, Blogs und Internetverzeichnissen erfasst haben. Sogar die Antwort auf eine Spam-Nachricht als Aufforderung zum Entfernen von einer Verteilerliste kann ein Trick sein, Sie zur Bestätigung Ihrer E-Mail-Adresse zu bewegen. Außerdem führen Spammer Verzeichnisangriffe durch, indem Sie Milliarden von Wort- und Zahlenkombinationen in eine E-Mail-Datenbank eingeben, um gültige Adresskombinationen zu ermitteln. Große E-Mail-Hosts, wie Hotmail und AOL, sind allein aufgrund des von ihnen abgewickelten E-Mail-Volumens besonders gefährdet.

Wie wird die Entdeckung vermieden?

Über Internetverbindungen nutzen Spammer die privaten Computer anderer Anwender, um Sammel-E-Mails millionenfach zu versenden. Sie nutzen Sicherheitslücken aus, um per Remote-Zugriff verborgene Software zu installieren, die private PCs in Mail- oder Proxy-Server verwandelt. Über diese „Spam-Zombies“ leiten sie Sammel-E-Mails und verschleiern so deren tatsächlichen Ursprung. Spam wird zur Vermeidung einer Entdeckung auch über Auslandsserver gesendet.

Wie funktionieren Phishing-Programme?

Phishing-Programme werden immer durchtriebener und täuschen selbst versierte Anwender. Phisher senden Spam-E-Mails unter der Vorgabe, dass diese von vertrauenswürdigen Unternehmen, wie Banken, eBay, Kreditkartenunternehmen und Versorgungsunternehmen, stammen. Sie fordern Sie auf, durch Klicken auf einen Link in der E-Mail auf ihre Nachricht zu antworten, um eine Transaktion zu bestätigen, einen Kontobetrug zu untersuchen oder Ihr Konto vor der Auflösung zu bewahren. Die E-Mails können sehr überzeugend sein und Logos sowie scheinbar authentische Daten enthalten. Über die Links werden die Anwender dann zu manipulierten Phishing-Websites geleitet, die auf den Diebstahl persönlicher Daten vom Verbraucher ausgelegt sind.

Was kann ich tun?

Sie können sich vor Spam in E-Mails und Instant Messages schützen, indem Sie die nachstehenden Regeln befolgen.

Installieren Sie ein umfassendes PC-Sicherheitspaket, und halten sie es auf aktuellem Stand. Ein E-Mail-Filter sowie eine PC-Spam-Blockiersoftware sind unbedingt erforderlich. Mit McAfee SecurityCenter können Sie Ihren Internetaktivitäten unbeschwert nachgehen, da Ihre Identität durch die Beseitigung von Viren, Spyware, E-Mail-Angriffen, Hackern und Datendieben und die automatische Sicherung wichtiger Dateien geschützt ist. Eine Firewall überwacht die PC-Aktivität und verhindert, dass Trojaner auf Ihrem Computer installiert werden.

Schützen Sie Ihre E-Mail-Adresse und Instant Message-ID. Veröffentlichen Sie diese nicht in Newsgroups, Chatrooms, Websites, Social Network-Seiten wie MySpace, Blogs oder Verzeichnissen von Online-Diensten. Richten Sie am besten zwei E-Mail-Adressen ein, eine für den tatsächlichen Gebrauch und eine für Newsgroups und Chats. Sie sollten Einblick in die Datenschutzbestimmungen und Formulare nehmen und Abmeldeoptionen nutzen.

Seien Sie äußerst vorsichtig beim Öffnen von Anhängen auf Ihrem PC, PDA oder drahtlosen Gerät. Konfigurieren Sie Ihre Antiviren-Software so, dass automatisch alle E-Mail- und Instant Message-Anhänge gescannt werden. Stellen Sie sicher, dass Ihr E-Mail-Programm Anhänge nicht automatisch öffnet oder Grafiken automatisch darstellt. Vergewissern Sie sich, dass das Vorschaufenster deaktiviert ist. Anweisungen hierzu finden Sie in den Sicherheitsoptionen oder im Einstellungsmenü Ihres Programms. Öffnen Sie niemals unangeforderte Geschäfts-E-Mails oder nicht erwartete Anhänge – auch nicht von Ihnen bekannten Personen.

Weisen Sie Ihre Kinder an, keine Online-Umfragen auszufüllen und sich nicht für Wettbewerbe oder Fan-Clubs zu registrieren. Sorgen Sie dafür, dass Ihre Kinder Sie darüber informieren, wenn sie Mitglied bei einer legitimen Website, wie Nickelodeon oder Cartoon Network, werden möchten, damit Sie die Datenschutzbestimmungen der Website lesen können.

Achten Sie auf Phishing-Mails. Klicken Sie nicht auf Links in E-Mails oder Instant Messages. Öffnen Sie stattdessen einen separaten Webbrowser, und rufen Sie die Website direkt auf. Sie können auch überprüfen, ob eine E-Mail legitim ist, indem Sie das Unternehmen direkt anrufen.

Wählen Sie einen Internet Service Provider (ISP), der auf hohe Sicherheit, wie Spamschutz- und Anti-Phishing-Verfahren, achtet (unter Spam.Abuse.Net finden Sie eine entsprechende Liste).

Antworten Sie nicht auf Spam. Auch wenn Sie auf Spam nur antworten, um diese Mails abzubestellen, könnte Ihnen dies nur noch mehr Spam-Mails einbringen. Senden Sie niemals Kreditkarten- oder Sozialversicherungsdaten bzw. andere private Informationen per E-Mail oder Instant Messaging.

Verwenden Sie eine komplizierte E-Mail-Adresse. Dadurch haben es Hacker schwerer, Ihre E-Mail-Adresse zufällig automatisch zu generieren oder Ihre Adresse für andere Bedrohungen zu missbrauchen. Verwenden Sie Buchstaben, Zahlen und andere Zeichen in einer einzigartigen Kombination. Ersetzen Sie nach Möglichkeit Buchstaben durch Zahlen. Beispiel für eine komplizierte E-Mail-Adresse: Tracy3Socc3r2@sampleemail.com.

Wählen Sie intelligente und sicher Kennwörter, die für Hacker schwer zu knacken sind. Verwenden Sie Großbuchstaben, Zahlen und Sonderzeichen – es sollten mehr als sechs Zeichen sein. Beispiel für ein sicheres Kennwort: Go1dM!n3.

Geben Sie keine privaten Daten in ein Popup-Fenster ein. Möglicherweise werden Sie von einem Phisher auf die Website eines seriösen Unternehmens geleitet, auf der aber dann von diesem Scammer ein nicht autorisiertes Popup-Fenster mit Feldern angezeigt wird, in die Sie Ihre persönlichen Daten eingeben sollen. Alle Daten, die Sie dort eingeben, werden zum Phisher gesendet. Mithilfe des Popup-Blockers in McAfee SecurityCenter können derartige Phishing-Angriffe verhindert werden.

McAfee GmbH
Ohmstr. 1
85716 Unterschleissheim
+49-89-3707 0
www.mcafee.de