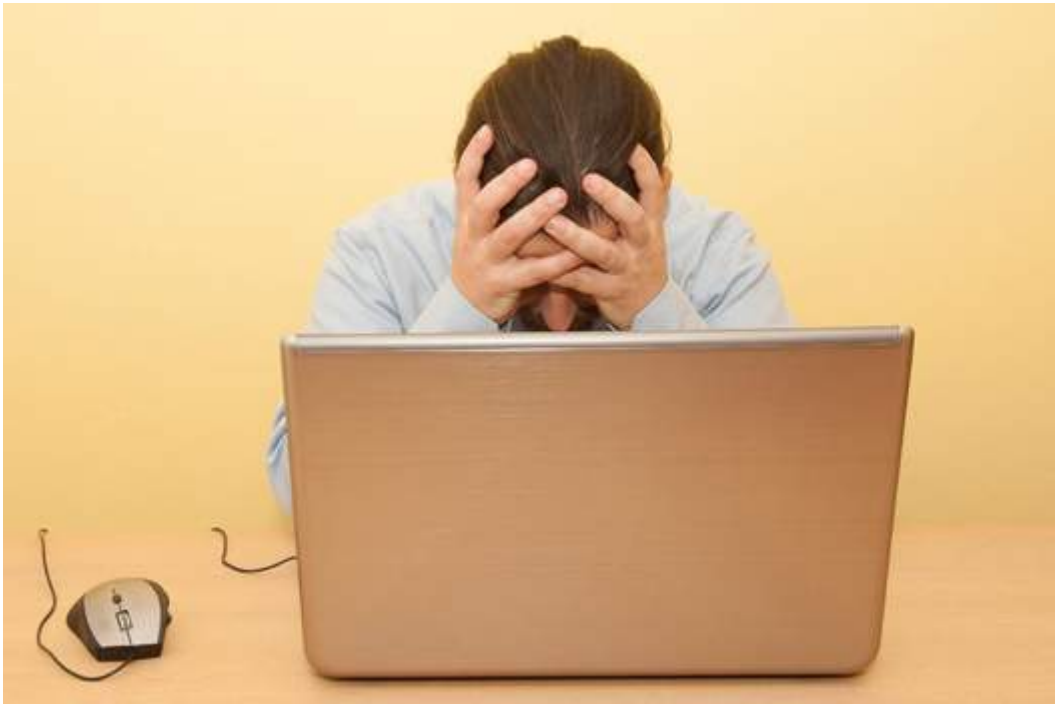
Video: Internetkriminalität – So schütze ich mich! >
< IT-Sicherheit für Berufsschüler

Falschmeldungen im Internet

Hoaxes und Kettenbriefe erkennen



Hoaxes sind ein weit verbreitetes Phänomen

Sie erhalten eine Mail von einem Kollegen, in der eine Stiftung angeblich Spendengelder für ein Katastrophengebiet sammelt. Mit jeder Weiterleitung würden ein paar Cent an die Betroffenen gehen. Bei solchen „Hoaxes“ handelt es sich um Falschmeldungen per Mail, die den leichtgläubigen Adressaten zum Weiterleiten an Freunde und Verwandte auffordern. Die unkontrollierte Weiterverbreitung macht Hoaxes zu einem ernsten Problem. Eine neue Variante sind Falschinformationen in sozialen Netzwerken, die im Ernstfall sogar eine potenzielle Gefahr für die Öffentlichkeit darstellen.

Ein gesundes Misstrauen hilft

„Hoaxes“ (aus dem Englischen für „schlechter Scherz“) sind massenweise weitergeleitete E-Mails, die ihre Empfänger dazu bringen wollen, die Nachricht wiederum an Freunde und Bekannte weiterzuleiten. Manchmal geht es um ein an Krebs erkranktes Kind aus Florida, bei dem für jedes Weiterleiten der Nachricht angeblich eine Spende ans behandelnde Krankenhaus gehen würde. Spam-Mails sind häufig als offizielle Mitteilung eines bekannten Unternehmens getarnt oder enthalten betrügerische Angebote. Malware-Spam enthält meistens sogar Schadprogramme, weshalb die Aufforderung zum Download keineswegs befolgt werden sollte. Frank Ziemann, IT-Berater und Betreiber der Homepage hoax-info.de, erklärt die begriffliche Unterscheidung: „Der Kettenbrief ist der klassische Verbreitungsmechanismus für Hoaxes.“ Seit 1997 beobachtet er das Phänomen und kennt mittlerweile alle erdenklichen Formen. „Es gibt kettenbriefartige Mails, die von mehreren Personen an wiederum mehrere Personen verbreitet

werden. Spam-Mails sind davon zu unterscheiden. Sie kommen von einem Absender und werden an viele gesendet“, so der Experte.

IT-Experte Frank Ziemann

© Frank Ziemann

Wer die Urheber solcher Falschmeldungen sind, bleibt häufig im Dunkeln. Oft stecken Kriminelle dahinter, die mit ihren Falschmeldungen großen Schaden anrichten können. IT-Experte Frank Ziemann betont, der beste Schutz sei vor allem ein gesundes Misstrauen des Empfängers: „In aller Regel kommen solche Hoaxes nicht von einer dubiosen Adresse, sondern von guten Bekannten und Verwandten, die solche Meldungen unreflektiert weiterversenden.“ Wenn der Absender eine Kollegin oder der eigene Nachbar ist, helfen auch keine Spam-Filter. Dann ist ein gewisses Maß an Skepsis angebracht, denn das Weiterleiten an noch mehr Menschen kann den Hoax zu einer digitalen Lawine heranwachsen lassen. Die Empfänger werden verunsichert, verschwenden womöglich unnötig Arbeitszeit und im schlimmsten Fall entstehen enorme Datenmengen auf Servern und Festplatten. Dabei gibt es eindeutige Hinweise, an denen sich ein Hoax im Posteingang erkennen lässt. Häufig enthalten sie eine Warnung, etwa vor einem gefährlichen Schadprogramm im Internet. Kurz darauf wird der Nutzer aufgefordert, die Meldung an seine persönlichen Kontakte weiterzusenden. Eine bekannte Firma oder gemeinnützige Organisation wird häufig als Urheber angegeben, um Seriosität vorzugaukeln. Zudem enthält der Hoax Aktualitätsangaben wie „gestern“ oder „kürzlich“, obwohl der betreffende Kettenbrief womöglich bereits Tage, Wochen, Monate oder sogar Jahre im Umlauf ist. Frank Ziemann empfiehlt beim Erhalt einer solchen Mail, sich im Zweifel gezielt zu informieren: „Wenn Sie eine verdächtige Nachricht erhalten, suchen Sie mit einer gängigen Suchmaschine nach ein paar prägnanten Stichworten aus der Mail im Internet. In der Regel kann ein Hoax über diesen Weg schnell entlarvt werden“, so Ziemann.

Bei gezielter Desinformation wird es gefährlich

Ein neuer Trend in sozialen Netzwerken wie Facebook und Twitter macht Falschmeldungen im Internet sogar zu einer Gefahr für die Öffentlichkeit. Bei dem rechtsextrem motivierten Amoklauf eines 18-Jährigen vor dem Olympia-Einkaufszentrum (OEZ) in München am 22. Juli haben vermeintliche Meldungen über weitere Schießereien die Bevölkerung verunsichert und die polizeiliche Arbeit erheblich beeinträchtigt. „Die Verbreitung von Desinformation hat sich als neuer Trend entwickelt“, erläutert Frank Ziemann. Zwar sei dies letztlich auch nur ein Einzelphänomen, welches in Krisensituationen aber verheerende Auswirkungen haben könne: „Für die Polizei sind solche Falschmeldungen natürlich besonders ärgerlich.“ Mit Falschmeldungen wird leider auch zunehmend fremdenfeindliche Propaganda betrieben. Dabei werden erfundene Geschichten über angebliches Fehlverhalten von Flüchtlingen oder Politikern verbreitet, die in sozialen Netzwerken die öffentliche Meinung beeinflussen können und dadurch noch gefährlicher sind. Auch moderne Kriegspropaganda bedient sich derartiger Mittel. Bundesinnenminister Thomas de Maizière (CDU) warnte kurz nach dem Amoklauf in München davor, Gerüchte und Falschinformationen über Soziale Medien zu verbreiten. Das deutsche Strafrecht stelle den Missbrauch von Notrufen und die Behinderung von Rettungsmaßnahmen unter Strafe. Nützliche Hinweise hingegen können die Sicherheitsbehörden bei ihrer Ermittlungsarbeit unterstützen. Schließlich nutzt auch die Polizei Soziale Medien wie Facebook und Twitter für ihre Kommunikation mit Bürgerinnen und Bürgern. Wer diese Kanäle verantwortungsvoll zu nutzen gewillt ist, kann unter Umständen zu mehr Sicherheit beitragen und die polizeiliche Aufklärung von Straftaten unterstützen.

Immer die Augen offen halten

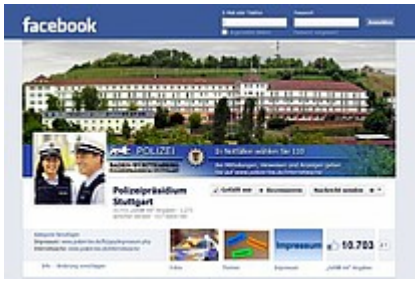
Ob nun beim Umgang mit verdächtigen E-Mails oder beim Posten und Tweeten – das World Wide Web bietet vielfältige Möglichkeiten der Kommunikation, aber eben auch des Missbrauchs. Hilfreich ist in solchen Fällen meist schon, die Augen offen zu halten und nicht jede Information sofort zu glauben. Betrüger nutzen die Gutgläubigkeit des Empfängers aus, um Hoaxes oder andere Formen von Falschinformationen über die neuen Medien zu verbreiten. Dabei beobachtet Frank Ziemann auch einen Trend: „Betrugsmails und Phishing-Mails kommen noch immer reichlich vor, aber die klassischen Mail-Hoaxes haben in letzter Zeit abgenommen." Das liegt auch daran, dass soziale Netzwerke als Kommunikationsmedien enorm an Relevanz gewonnen haben. „Die Prozesse gehen mit den gängigen Kommunikationsmedien", folgert der IT-Experte. Die Herausforderung für die Sicherheitsbehörden bleibt der souveräne Umgang mit den modernen Kommunikationsformaten. Alle Menschen können diese Medien nutzen – ob in guter oder böser Absicht. Information und Aufklärung können dabei helfen, die gezielte Verbreitung von Fehlinformationen einzudämmen. AL (28.10.2016)

Folgende Artikel könnten Sie auch interessieren:

- Die Polizei auf Facebook und Twitter
- Fakt oder Fake?
- Polizei und Social Media
- Malware und Spyware - „Stars" der Internetkriminalität

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil



Das Polizeipräsidium Stuttgart hat über 46.000 Facebook-Fans

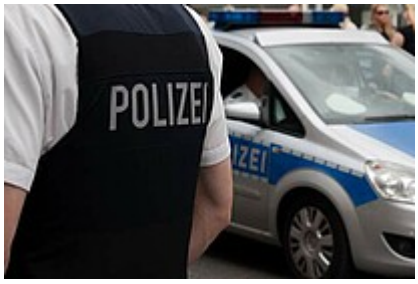
Die Polizei auf Facebook und Twitter

Für die Polizeipräsidien sind Soziale Medien ein wichtiger Kanal, um...[mehr erfahren]

Eltern müssen ihre Kinder beim Medienkonsum begleiten

Mit Verboten kommt man nicht weit

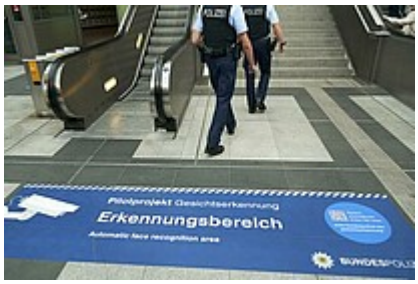
Martin Lorber ist Pressesprecher des Spieleherstellers Electronic...[mehr erfahren]



Nutzen und Risiken richtig einschätzen

Polizei und Social Media

Viele Menschen finden es spannend, wenn in ihrer näheren Umgebung ein...[mehr erfahren]



Berliner Pilotprojekt zur Gesichtserkennung erfolgreich

Wie Computer lernen, Menschen zu erkennen

Biometrische Systeme wie Fingerabdruck- oder Gesichtsscanner werden...[mehr erfahren]

Hilfe von Jugendlichen für Jugendliche

Erste-Hilfe-App bei Cybermobbing

Beleidigungen auf Facebook oder peinliche Fotos, die über WhatsApp...[mehr erfahren]
