



## Sicherheit

### Sicherheitshinweise zu Phishing-E-Mails

Um nicht zu Opfern der Datenfischer zu werden, sollten Sie unbedingt folgende vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Sicherheitsmaßnahmen beherzigen:

#### **Banken oder seriöse Einrichtungen fordern ihre Kunden niemals per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf**

Geldinstitute, Online-Auktionshäuser wie eBay, aber auch sonstige seriöse Wirtschaftsunternehmen und IT-Dienstleister wissen, dass E-Mails von Betrügern leicht gefälscht werden können. Daher werden sie ihre Kunden **niemals** per E-Mail dazu auffordern, darin angeführte Links anzuklicken und dort vertrauliche Daten einzugeben. Gleiches gilt für Beschäftigte des HRZs der Universität Bielefeld. Auch Sie werden Sie niemals dazu auffordern, vertrauliche Informationen wie Passworte oder ähnliches preiszugeben. Wenn Sie eine derartige E-Mail erhalten, dann können Sie davon ausgehen, dass es sich um einen Phishing-Angriff handelt. Wenn Sie unsicher sind, dann setzen Sie sich telefonisch oder brieflich mit dem vermeintlichen Absender in Verbindung, aber verfolgen Sie keinesfalls die in der Nachricht angegebenen Internetlinks.

Das Gleiche gilt für dubiose Telefonate: Seriöse Geschäftspartner oder Banken werden sich niemals von sich aus telefonisch bei Ihnen melden und Sie zur Eingabe von Passwörtern, PIN oder TAN über die Tastatur oder per Sprachcomputer auffordern!

#### **Bringen Sie Ihre Software immer auf den aktuellen Stand**

Sicherheitslücken in Programmen, insbesondere in Browsern (z. B. Internet Explorer, Firefox, Safari, Opera) und E-Mail-Klienten (z. B. Outlook, Thunderbird, Apple-Mail), können von Daten Fischern ausgenutzt werden. Die meisten Hersteller steuern dagegen, in dem sie ihre Software laufend aktualisieren und bekannt gewordene Lücken schließen. Sie sollten diese Aktualisierungen („Patches“) unbedingt so rasch wie möglich von den Webseiten der Hersteller herunterladen und installieren. Über neue Patches informieren viele Hersteller über automatische Update- und Warndienste, wichtige Neuerungen erfahren Sie auch im Newsletter „Sicher Informiert“, den das [BÜRGER-CERT des BSI](#) alle zwei Wochen veröffentlicht.

#### **Überprüfen Sie den Sicherheitsstatus von Webseiten, auf denen Sie persönliche Informationen eingeben**

Dabei sollten Sie besonders auf zwei Punkte achten:  
Auf gesicherten Seiten erscheint in der Statuszeile des Browsers ein Schlosssymbol. Dieses Symbol zeigt an, dass bei der Übertragung von Informationen das Verschlüsselungsverfahren SSL zum Einsatz kommt. Wenn Sie auf das Schlosssymbol klicken, öffnet sich ein Fenster („Zertifikat“) mit Informationen über den Betreiber der Webseite. Der dort angegebene Namen der Webseite muss mit jenem in der Statuszeile übereinstimmen. Außerdem muss das Zertifikat von einer anerkannten Stelle ausgestellt

worden sein. Es existiert mittlerweile eine große Zahl an privaten wie öffentlichen Anbietern von Zertifikaten. Die [Bundesnetzagentur](#) ist als Behörde zuständig und veröffentlicht auf ihrer Webseite die Namen jener Anbieter, die von ihr geprüft wurden. Ihr Browser zeigt eine Warnmeldung an, wenn ein Zertifikat abgelaufen ist oder eine unsichere Herkunft hat.

Achten Sie darauf, dass der in der Adresszeile angegebene URL mit „https“ und nicht wie sonst üblich mit „http“ beginnt – das ist ein starkes Indiz dafür, dass eine durch SSL gesicherte Verbindung aufgebaut wurde. Leider können Betrüger auch das „https“ in der URL fälschen. Als Sicherheitscheck hilft es hier, nach einem Klick mit der rechten Maustaste den Bereich „Seiteninformationen“ aufzurufen und die Quelle dort nachzuschlagen.

### **Beachten Sie die generellen Sicherheitsregeln, die für das Internetsurfen und den E-Mail-Verkehr gelten**

Klicken Sie generell niemals auf in E-Mails enthaltene Links, sondern tippen Sie die Internetadressen gewünschter Seiten immer manuell ein. Antworten Sie ferner niemals auf E-Mails, in denen Sie zur Eingabe von PIN oder TAN bzw. zur Angabe von Benutzernamen oder Passwörtern aufgefordert werden – etwa mit der Behauptung, dass dadurch Sicherheitslücken geschlossen werden sollen.

Schalten Sie die Funktion „Aktive Inhalte ausführen“ generell aus. Wenn Sie darauf nicht verzichten wollen, so stellen Sie über die entsprechende Funktion in den Sicherheitseinstellungen zumindest sicher, dass Ihr Browser in jedem Einzelfall bei Ihnen anfragt, ob Aktive Inhalte ausgeführt werden dürfen.

### **Öffnen Sie E-Mails und darin enthaltene Anhänge nur dann, wenn Sie aus vertrauenswürdiger Quelle stammen**

Setzen Sie eine Firewall und Virenschutzsoftware ein und bringen Sie diese regelmäßig auf den aktuellen Stand.

Achten Sie darauf, dass Sie auch die Softwareaktualisierungen für Ihr Betriebssystem und andere von Ihnen eingesetzte Programme laufend installieren oder nutzen Sie automatische Update-Dienste.

Wenn Sie befürchten, dass Sie einem Phishing-Angriff zum Opfer gefallen sind, bewahren Sie Ruhe und kontaktieren Sie das dementsprechende Unternehmen bzw. die Hochschule. Die für Sicherheitsfragen zuständigen Mitarbeiter können den Vorfall verfolgen und prüfen, ob Schaden entstanden ist.