Schutzmaßnahmen gegen Phishing

Normalerweise wirst du nicht selbst mit Banken, Versicherungen oder Versandhäusern zu tun haben – dafür sind meist die Eltern zuständig. Vielleicht hast du aber einen eigenen Rechner, bekommst Werbemail oder hast mit Zustimmung deiner Eltern schon online eingekauft. In jedem Fall solltest du dich rechtzeitig über die Methoden krimineller Datenfischer informieren, denn mit 18 bist du voll geschäftsfähig und kannst selbst zum Opfer eines Online-Betrugs werden! Deshalb solltest du schon jetzt folgende Schutzmaßnahmen berücksichtigen.

- **Regel 1: Bringe deine Software immer auf den aktuellen Stand!** Sicherheitslücken in Programmen, insbesondere in Browsern, können von Datenfischern ausgenutzt werden. Die meisten Hersteller steuern dagegen, in dem sie ihre Software laufend aktualisieren und bekannt gewordene Lücken schließen. Du solltest 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 erfährst du auch im Newsletter „Sicher • Informiert“ , den das BÜRGER-CERT des BSI alle zwei Wochen veröffentlicht: www.buerger-cert.de.

- **Regel 2: Überprüfe den Sicherheitsstatus von Webseiten, auf denen du persönliche Informationen eingibst! Dabei solltest du besonders auf zwei Punkte achten:**

1. 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 du auf das Schlosssymbol klickst, 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 gibt mittlerweile eine große Zahl an privaten und öffentlichen Anbietern von Zertifikaten. Die Bundesnetzagentur ist als Behörde zuständig und veröffentlicht auf ihrer Webseite die Namen jener Anbieter, die von ihr geprüft

wurden. Dein Browser zeigt eine Warnmeldung an, wenn ein Zertifikat abgelaufen ist oder eine unsichere Herkunft hat.

2. Achte darauf, dass der in der Adresszeile angegebene URL mit "https" und nicht wie üblich mit "http" beginnt – das ist ein sicheres Anzeichen 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.

Regel 3: Banken oder seriöse Firmen fordern ihre Kunden niemals per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf!

- Banken, Versicherungen, Online-Auktionshäuser wie eBay, aber auch andere seriöse Wirtschaftsunternehmen 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.
- Wenn du eine derartige E-Mail erhältst, dann kannst du davon ausgehen, dass es sich um einen Phishing-Angriff handelt. Wenn du unsicher bist, dann bitte deine Eltern, sich mit eurer Bank oder der jeweiligen Firma in Verbindung zu setzen, um zu klären, ob die Nachricht nicht vielleicht doch echt war.
- Klick auf keinen Fall auf die Internetlinks in der gefälschten Nachricht! Das Gleiche gilt natürlich auch für Telefonate: Seriöse Firmen oder Banken werden sich niemals von sich aus telefonisch bei deiner Familie melden und dich zur Eingabe von Passwörtern, PIN oder TAN über die Tastatur oder per Sprachcomputer auffordern!

Regel 4: Beachte die allgemeinen Sicherheitsregeln, die für das Internetsurfen und den E-Mail-Verkehr gelten!

- Klicke generell niemals auf in E-Mails enthaltene Links, sondern tippe die Internetadressen der Seiten immer von Hand ein!
- Reagiere nicht auf vermeintliche Anrufe eurer Bank, in denen du zur Eingabe von PIN oder TAN aufgefordert wirst – etwa mit der Behauptung, die Kreditkarte deiner Eltern sei verloren gegangen.

- Schalte die Funktion „Aktive Inhalte ausführen“ in deinem Mailprogramm generell aus. Wenn du darauf nicht verzichten willst, so stelle über die entsprechende Funktion in den Sicherheitseinstellungen sicher, dass dein Browser in jedem Einzelfall anfragt, ob Aktive Inhalte ausgeführt werden dürfen.
- Öffne E-Mails und darin enthaltene Anhänge nur dann, wenn sie aus vertrauenswürdiger Quelle stammen.
- Setze deine Firewall und Virenschutzsoftware ein und bringe sie regelmäßig auf den aktuellen Stand.
- Achte darauf, dass du auch die Softwareaktualisierungen für dein Betriebssystem und andere Programme laufend installierst oder nutze die automatischen Update-Dienste.

Regel 5: Bitte deine Eltern Bank möglichst rasch zu reagieren, wenn du einem Phishing-Angriff zum Opfer gefallen bist!

- Die für Sicherheitsfragen zuständigen Mitarbeiter in eurer Bank oder Versicherung können den Vorfall verfolgen und prüfen, ob Schaden entstanden ist.
- Falls tatsächlich schon Geld überwiesen worden ist, dann wenden sich deine Eltern besser sofort an die Polizei.