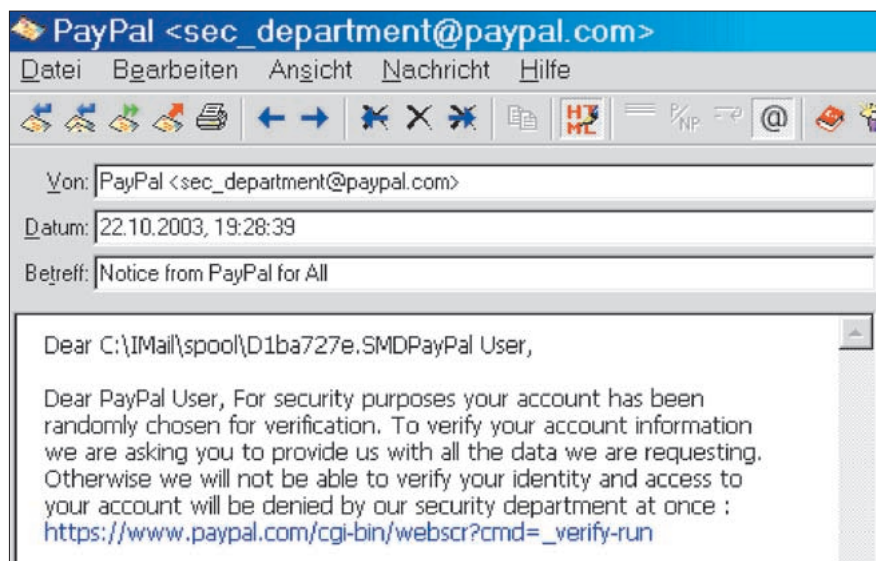


Achtung: Netzbanditen

Schützen Sie sich und Ihre Kinder vor Netzverbrechern, die im Schutz der Anonymität lügen, stehlen und betrügen. Der PCtipp zeigt, wie Sie Gefahren erkennen und ihnen vorbeugen.



Betrug in Rein-kultur: Solche Mails – hier eine gefälschte von PayPal – sollten Sie sofort löschen

SICHERHEITS-TIPPS

Schützen Sie sich

- Schliessen Sie alle Sicherheitslücken in Windows (mit START/WINDOWS UPDATE).
- Schützen Sie sich vor Viren und Spam (siehe Seite 26–31 in dieser Ausgabe).
- Inhaltsfilter (z. B. von Dritt-anbietern wie Symantec www.symantec.ch, Webwasher www.webwasher.de oder Surfcontrol www.surfcontrol.com) schützen vor schädlichen Inhalten.
- Hüten Sie persönliche Daten. Dazu gehören Ihr Name, Ihre Adresse, Ihr Geburtsdatum und Ihre Kreditkarten- und andere Nummern.
- Prüfen Sie Internetgeschäfts-partner auf Herz und Nieren: Rufen Sie die angegebenen Telefonnummern an, kontrollieren Sie, ob die Adresse tatsächlich existiert.
- Senden Sie nie Geld im Voraus und verzichten Sie im Zweifelsfall auf einen Kauf. Wer Geld per schnellem Geldtransfer verlangt, macht sich verdächtig und verdient einen zweiten Blick des Käufers.

von Bruno Habegger

Quizfrage: Sie erhalten eine Mail, in der Sie aufgefordert werden, Ihre Kontodaten beim Provider XY oder bei der Online-Bank YZ zu erneuern. Was tun Sie? A: Sie ignorieren diese Mail. B: Sie tun wie geheissen und rufen mit dem in den E-Mail-Text eingebetteten Link die entsprechende Website auf und ändern die Daten. Sie ahnen es: Antwort B führt Sie schnurstracks in die Pleite.

LINKS

Wichtige Adressen

Phishing
www.antiphishing.org

Internet Content Rating
www.icra.org/_de

Microsoft Sicherheit
www.microsoft.com/security

Schutz vor Anlagebetrug
www.stoppbetrug.ch

Computerbetrug
www.computerbetrug.de

Identitätsdiebstahl
www.identitytheft.org

Computer Security Schweiz
www.computer-security.ch

Phishing nennt sich der in letzter Zeit wieder gehäuft auftretende Trick. Dabei erhalten Anwender angeblich seriöse E-Mails von einer Bank, von eBay, PayPal oder anderen Unternehmen, die aber in Tat und Wahrheit von Betrügern verschickt werden.

Wer auf den mitgelieferten Link klickt und einen Internet Explorer ohne Sicherheitsaktualisierungen (abzuholen unter <http://windows.update.microsoft.com>) verwendet, sieht eine täuschend echte Seite mit der scheinbar korrekten Internet-adresse. In Wirklichkeit ist es aber eine Fälschung, die von Ihnen Passwörter und Kreditkartendaten erfassen möchte.

Diese Masche erinnert an die Sicherheitsgrundregel Nummer eins: *Seien Sie misstrauisch!* Keine ehrliche Firma, kein ernst zu nehmender Provider fragt Sie per E-Mail nach Ihrem Passwort oder fordert Sie gar auf, Ihre Kontodaten neu einzugeben. Lesen Sie E-Mails immer ganz genau und antworten Sie nie auf Mails von unbekannten Absendern.

Auch ein Zugangsfilter kann Sie – und Ihre Kinder – vor Kriminellen aus dem Internet schützen. Gerade im Umfeld von Pornoseiten besteht erhöhte Dialer-, Viren- und Wurm-

gefahr. Und auch Betrüger tummeln sich gehäuft auf solchen Seiten. So schalten Sie den Inhaltsfilter des Internet Explorers ein: Gehen Sie über EXTRAS zum Menü INTERNETOPTIONEN/INHALTE/INHALTSRATGEBER. Falls dieser noch nicht aktiviert ist, tun Sie das mit AKTIVIEREN. Tragen Sie die gewünschten URLs unter «Gebilligte Sites» ein und deaktivieren Sie unter ALLGEMEIN «Zugang auf ungefilterte Sites zulassen». Den Zugriff auf andere URLs und den Inhaltsratgeber verhindern Sie mittels Passwort. Details finden Sie auf <http://support.microsoft.com> in der Knowledge Base, Artikelnummer 310401.

Auch Internetauktionen sind nicht ungefährlich. Prüfen Sie deshalb jedes Angebot ganz genau. Es kommt z. B. immer wieder vor, dass Handy-Schachteln zum Kauf angeboten werden – allerdings ohne Handy. Der Hinweis ist zwar vorhanden, aber gut versteckt. Zahlen Sie nie Geld im Voraus ein. Nutzen Sie ausschliesslich die von der Auktionsseite empfohlenen Treuhanddienste. Geben Sie persönliche Daten wie Kreditkartennummern nur preis, wenn Sie die Identität der Gegenseite geprüft haben oder Sie von deren Seriosität absolut überzeugt sind.

MINITIPP INTERNETVERBINDUNG

Modemstatus anzeigen

Möchten Sie in der Windows-Taskleiste den Status Ihrer Internetverbindung sehen? Unter Windows 2000 und XP ge-



Werden Daten übertragen, blinken die kleinen Symbolmonitore

hen Sie zu START/EINSTELLUNGEN/NETZWERKVERBINDUNGEN, klicken mit Rechts auf die Verbindung und im Kontextmenü auf EIGENSCHAFTEN. Im Register ALLGEMEIN aktivieren Sie «Symbol bei Verbindung im Infobereich anzeigen». Unter Windows 9x und Me öffnen Sie im ARBEITSPLATZ das DFÜ-NETZWERK und die EIGENSCHAFTEN Ihrer Modemverbindung, klicken auf KONFIGURIEREN und haken unter OPTIONEN «Modemstatus anzeigen» an. (sal)