

Es ist schnell mal passiert, das man sich beim eingeben von Internetadressen vertippt (z.B. aus Ebay.de wird Ebey.de, aus Neckermann.de wird Neckmann.de) Der Internetbrowser sagt dann nicht falsche Adresse, bittet um eine neue Eingabe, sondern stattdessen gelangt man oft auf andere Seiten und das kann böse Folgen haben. So können Sie sich schützen.

Seitenbesetzer

Es gibt Internetnutzer die gezielt Seiten mieten die sehr oft in der Adresszeile einen falsch geschriebenen prominenten Namen haben. Diesen Trend nennt man im englischen „Typosquatting“, das heißt übersetzt: Das Hocken auf Tippfehlern. Nach Erfahrung von Experten sind bei Typosquattern vor allem Seiten von Fluglinien, bekannten Internetmedien und Onlineshops beliebt. Bei Schülern und Studenten geraten aber gern beliebte Webangebote ins Visier.

Gelddruckmaschine

Ohne selbst viel Geld investieren zu müssen, lässt sich mit Typosquatting ganz legal Geld verdienen. Das Registrieren einer Seite auf seinen eigenen Namen kostet pro Jahr wenige Dollar. Die Seiten mit Rechtschreibfehlern in der Adresszeile werden dann so gestaltet, dass große Suchmaschinentreiber darauf Werbebanner platzieren. Yahoo, Google und Co. packen im Kundenauftrag Anzeigen auf Internetseiten, die auch thematisch etwas mit der Werbung zu tun haben.

Die Menge macht es

Elektroware wird dann auf Seiten zu Computerthemen beworben, Fischfutterwerbung findet sich auf Webseiten mit Aquaristikthemen. Wird die platzierte Werbung angeklickt, fließt immer ein kleiner Cent-Betrag an den Eigentümer der Internetseite. Und weil sich sehr viele Menschen vertippen, wird auch entsprechend oft auf die Werbebanner geklickt.

Graubereich

Auch eine von den Tippfehler-Hockern gern angewandte Masche: Sie lassen Seiten registrieren, deren Namen den Anbietern bekannter Markenartikel ähneln. Auf der Seite mit kleinem Fehler in der Adresszeile werden dann Plagiate dieser Markenartikel angeboten.

Drive-by-Download

Weniger harmlos dagegen sind solche Webseiten mit Rechtschreibfehler, auf denen Internetgauner Schadprogramme parken. Die können sich schon auf dem eigenen Computer einnisten, wenn man die entsprechende Seite nur besucht. Also nach einem Tippfehler beispielsweise. Dazu nutzen die Hacker Lücken im Internetbrowser aus. Das Perfide: Als Nutzer bemerkt man nichts von diesen so genannten Drive-by-Downloads.

4456 3990 9998 9982

Die Schadprogramme spähen dann beispielsweise Passwörter oder auch Kreditkartendaten aus, indem sie alle Tastatureingaben protokollieren und dann an den Hacker senden. Tippfehler passieren immer wieder, vor den Drive-by-Downloads kann man sich aber schützen. So sollte man einen möglichst aktuellen

Vertippt bei Internetadressen – Vorsicht Falle!

2008

Internetbrowser wie den Firefox 3 von Mozilla oder den Internet Explorer 7 von Microsoft nutzen. Hier sind die Einfallstore gegen Hacker relativ dicht. Zusätzlich hilft noch ein ständig aktualisierter Virenschanner gegen Schadprogramme.