

Phishing – Was ist das?

Bei sogenannten „Phishing-Attacken“ versuchen Betrüger im Internet mit gefälschten eMails und Internet-Sites geheime Informationen von Internet-Nutzern zu erschleichen: Eine eMail scheint von einem seriösen Anbieter zu stammen; der Absender und der Inhalt der eMail ist jedoch gefälscht. Der Empfänger der eMail wird mit plausibel klingenden Worten aufgefordert, eine bestimmte (gefälschte) Web-Site zu besuchen und dort geheime Daten einzugeben. Dies erfolgt in der Regel als Link in der Phishing eMail. Die Phishing Web-Site hat meist eine sehr ähnliche Adresse und Oberfläche, wie die Web-Site des seriösen Anbieters. Gibt der Internet-Nutzer auf dieser Web-Site seine Daten ein, so kann der Betrüger diese Daten – meist zum finanziellen Nachteil des Internet-Nutzers - missbrauchen.

Bei solchen „Phishing-Attacken“ werden z.B. Bankkunden aufgefordert, auf der nachgestellten eBanking Login-Seite Kundennummer und PIN einzugeben. In einem darauf folgenden Formular werden dann Informationen rund um die Bankverbindung des Kunden abgefragt: z.B. Konto-Nummer, Kreditkarten-Nummer, PINs und TANs etc.

Mitarbeiter der Bank werden Sie niemals auffordern PIN/TAN, Konto oder Kundennummer anzugeben!

Phishing-Mail – Was tun?

Sollten Sie eine entsprechende Mail erhalten sperren Sie Ihren NetKey und setzen Sie sich Bitte sofort mit uns in Verbindung.

Außerhalb unserer Geschäftszeiten können Sie unter der Hotline-Nummer (0180) 50 53 111 (12 Cent/min. aus dem deutschen Festnetz) anrufen. Diese ist täglich von 8:00 bis 24:00 Uhr besetzt.