NEWSLETTER
Phishing

Was ist Phishing?
Phishing beschreibt Datendiebstahl oder das Ausspionieren von Daten.

Was wird „gephisht“?
Meistens haben es Kriminelle auf Passwörter abgesehen, z. B. bei Bankkonten.

Wie wird „gephisht“?
- Über Spam-Mails können Opfer von Phishing-Angriffen auf beinahe perfekt nachgeahmte Webseiten weitergeleitet werden. Dort werden die vom Opfer eingegebenen sensiblen Daten von Cyber-Kriminellen ausgelesen.
- Vorwand ist häufig eine Aktualisierung der persönlichen Daten unter dem Druck von beispielsweise dem baldigen Ablauf einer Kreditkarte.

Wie kann man sich vor Phishing schützen?
Der beste Schutz vor Phishing ist der Mensch selbst.
Aufmerksamkeit und Skepsis im Internet sind das A und O!
Bei E-Mails sollten vor allem auf folgende Dinge geachtet werden:

- Gefälschte E-Mail Adresse
- Abfrage vertraulicher Daten
- Links zu gefälschten Webseiten
- Sprachliche Ungenauigkeiten
- Vorgetäuschter, dringender Handlungsbedarf (Druck!)

Das Wichtigste in Kürze

Ziel von Kriminellen	Arbeitsweise	Bester Schutz
Zugangsdaten wie Passwörter, Transaktions-nummern usw.	Im Internet: Täter versenden E-Mails oder treten in sozialen Netzwerken als vertrauenswürdige Person auf. Am Telefon: Betrüger tarnen sich als Mitarbeitende. Per Post: Empfänger soll online ein Sicherheits-passwort vergeben, oft VISA/Mastercard.	• Aufmerksam bleiben • Echtheit hinterfragen • Im Zweifel Absender kontaktieren (2. Kanal)

Noch Fragen?
Wenden Sie sich gerne an Ihre Ansprechperson der Informationssicherheit: isb@hs-kehl.de

Tipp: Überprüfen Sie, ob Sie selbst auf Phishing-Versuche hereinfallen würden!
- bereitgestellt vom Karlsruher Institut für Technologie