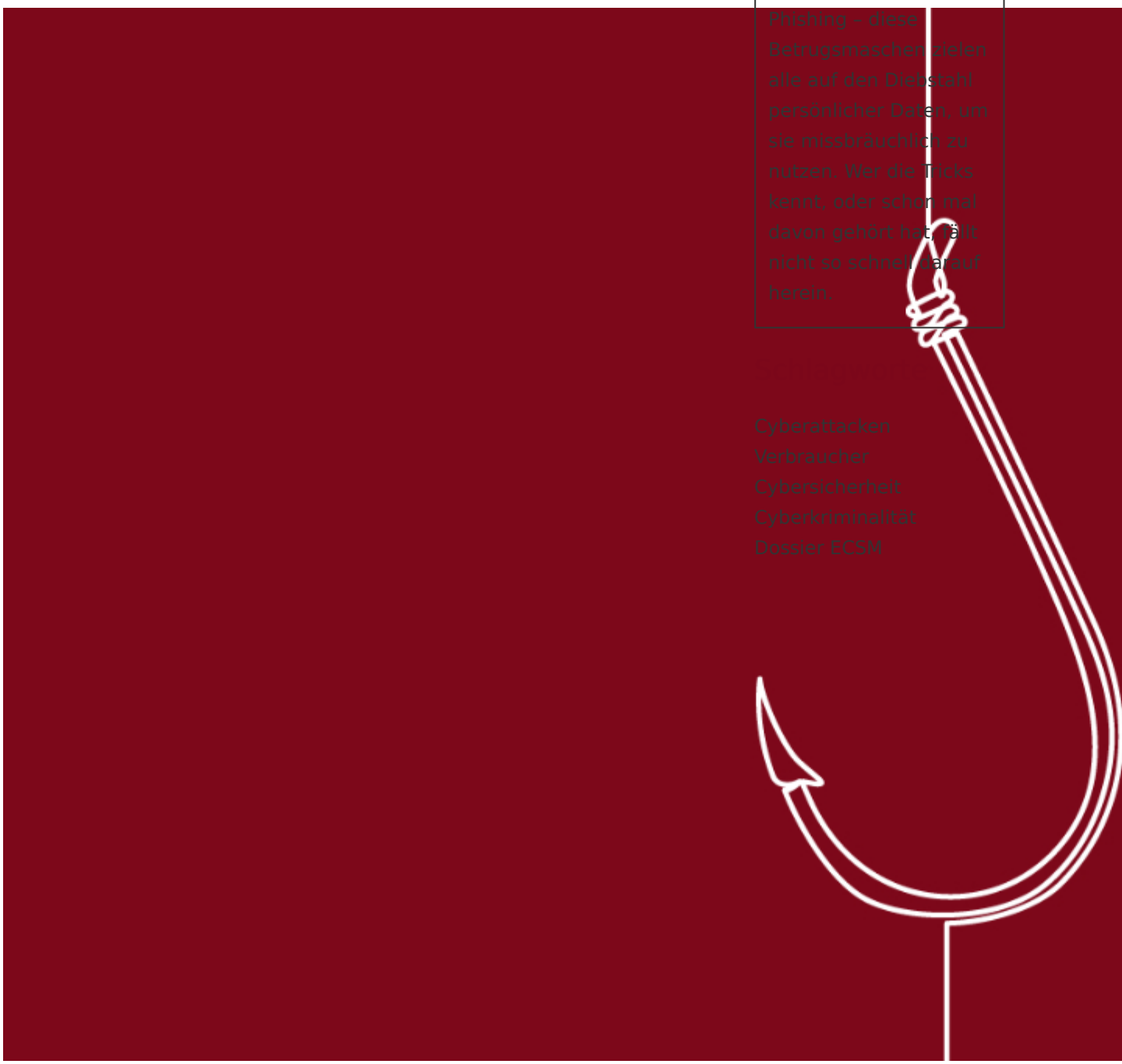
Smishing, Vishing, Phishing: Achtung, Datenklau!

19.10.2018
von Kathleen Altmann

Kurzgefasst

Smishing, Vishing und Phishing – diese Betrugsmaschen zielen alle auf den Diebstahl persönlicher Daten, um sie missbräuchlich zu nutzen. Wer die Tricks kennt, oder schon mal davon gehört hat, fällt nicht so schnell darauf herein.

Cyberattacken
Verbraucher
Cybersicherheit
Cyberkriminalität
Dossier ECSM



Der Begriff Phishing ist schon bei vielen bekannt, aber wer hat schon von Smishing oder Vishing gehört? Was sich zunächst harmlos anhört, zielt eigentlich nur darauf ab, den Empfänger zu erleichtern – und zwar um seine sensiblen Daten oder letztlich um sein Geld.

Betrug per SMS: Smishing

Beim Smishing, geht es um Phishing per SMS. Der Empfänger der Textnachricht wird dazu aufgefordert, einem Link zu folgen oder eine Telefonnummer anzurufen, um das eigene Konto zu „prüfen“, zu „aktualisieren“ oder zu „reaktivieren“. Das führt das potenzielle Opfer dann geradewegs zu einer gefälschten Webseite oder die Telefonnummer zu einem Kriminellen, der sich als Mitarbeiter des echten Unternehmens ausgibt.

Unerbetene Anrufe: Vishing

Beim Vishing – der Begriff setzt sich zusammen aus „Voice“ und „Phishing“ – soll das Opfer am Telefon dazu verleitet werden, seine Daten herauszugeben oder direkt Geld an die Kriminellen zu überweisen. Kriminelle recherchieren vorab in den sozialen Medien persönliche Informationen des potenziellen Opfers und leiten es damit in die Irre. Daher sollte man Anrufern nicht nur deshalb vertrauen, weil sie solche persönlichen Details kennen. Im Zweifel lässt man sich die Telefonnummer geben und verspricht einen Rückruf. So gewinnt man Zeit und kann die Telefonnummer der Organisation selbst nachprüfen. Natürlich darf nicht die im Display angezeigte Nummer zurückgerufen werden, denn genau diese kann gefälscht sein.

Gefährliche E-Mails: Phishing

Das klassische Phishing ist dagegen schon bekannter: Mit betrügerischen E-Mails soll der Empfänger verleitet werden, persönliche, finanzielle oder sicherheitsbezogene Informationen preiszugeben. Meist sehen diese E-Mails der Korrespondenz mit der eigenen Bank sehr ähnlich, die bekannten Logos werden benutzt, das Layout und sogar der Tonfall gleicht dem der echten E-Mails. Kriminelle bauen hier vor allem darauf, dass die Leser häufig vielbeschäftigt sind und deshalb E-Mails nur oberflächlich lesen. Sie vermitteln den Eindruck, es sei dringend und verlangen, dass ein Anhang geöffnet oder auf einen Link geklickt wird. Besonders bei mobilen Endgeräten, wie dem Mobiltelefon oder Tablet, kann es schwierig sein, den Phishing-Versuch zu erkennen.

Wie man sich schützen kann

Generell gilt: Keine Eile, keine Hektik! Wichtig ist es, sich Zeit zu nehmen, sich nicht unter Druck setzen zu lassen. Links, Anhänge und Bilder sollten nicht geöffnet werden, ohne vorher den Absender zu prüfen. Das gilt sowohl für Textnachrichten, als auch für E-Mails. Die Adresse kann manuell im Browser eingegeben werden.

Übrigens fragen Banken niemals, weder per Textnachricht noch per Telefon oder E-Mail nach Onlinebanking-Passwörtern, PINs der Kredit- oder Debitkarte oder nach anderen Sicherheitsmerkmalen und fordern auch nie dazu auf, Geld auf ein anderes Konto zu überweisen.

Für den Fall, dass man vermutet, doch Opfer einer solchen Betrugsmasche geworden zu sein, sollte umgehend die eigene Bank kontaktiert werden, um einen Schaden weitgehend abzuwenden. Dass Kriminelle versuchen, an sensible Daten zu gelangen, kann nicht verhindert werden. Aber besondere Wachsamkeit und die Kenntnis der Tricks senken zumindest das Risiko eines Schadens.