Beim Social Engineering werden Nutzer manipuliert, indem die Angreifer deren Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausnutzen.

Sie als Angegriffene sollen dadurch dazu verleitet werden, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware zu installieren, auf Ihrem privaten Gerät oder einem Dienstcomputer im Behördennetzwerk. Das zentrale Merkmal beim Social Engineering besteht darin, Sie über die Identität und die Absicht des Täters zu täuschen.

Phishing von Passwörtern

Durch täuschend echt wirkende E-Mails sollen Sie dazu gebracht werden, auf einen Link zu klicken und auf der ebenso gefälschten Zielseite Passwörter oder Anmeldeinformationen einzugeben, die dann vom Angreifer abgegriffen werden können.

Spear-Phishing

Hierbei handelt es sich um eine besonders trickreiche Variante des Phishing, die die potenzielle Trefferquote noch erhöht. Die Angreifer schneiden ihre gefälschten E-Mails nach vorausgegangener Recherche speziell auf kleine Gruppen oder einzelne Personen oder Mitarbeiter zu.

CEO Fraud

Bei dieser Betrugsmasche versuchen Kriminelle, Entscheidungsträger oder befugte Mitarbeiter in Unternehmen und Behörden zu täuschen, damit diese vermeintlich korrekte Überweisungen von Geldbeträgen veranlassen.

www.thueringen.de

digitale Services
verwaltung.thueringen.de

Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©weerapat1003 (Titel), ©chinnarach (S. 5), ©ronniechua (innen oben), ©calypso77 (innen unten)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Social Engineering erkennen und verhindern

Wie wir von manipulativen Angreifern getäuscht werden und was man dagegen tun kann

Informationssicherheit

Hochprofessionelle Cyberkriminelle gehen bei ihren Aktivitäten äußerst geschickt vor. Sie sammeln harmlose private Informationen eines Nutzers, um damit Betrug im großen Stil zu ermöglichen oder sensible dienstliche Informationen auszuspähen. Dagegen sind Sie nicht wehrlos: Wenn Sie das richtige Gefahrenbewusstsein entwickeln, gibt es gegen jede dieser Maschen einfache Mittel.

Zurückhaltung bei persönlichen Angaben

Überlegen Sie genau, welche persönlichen Informationen Sie in sozialen Netzwerken mitteilen. Ihre Angaben werden von Kriminellen gesammelt. Sie missbrauchen diese als Hilfsmittel für Täuschungsversuche.

Keine „Daten-Postkarten“ schreiben

Nennen Sie niemals gemeinsam Zugangsdaten und dazugehörige Passwörter zusammen in einer E-Mail. Dieser Übertragungsweg ist so unsicher wie eine Postkarte. Trennen Sie die Daten auf verschiedene Medien auf, zum Beispiel senden Sie den Nutzernamen per E-Mail und teilen das Passwort telefonisch mit.

Zurückhaltung bei dienstlichen Vorgängen

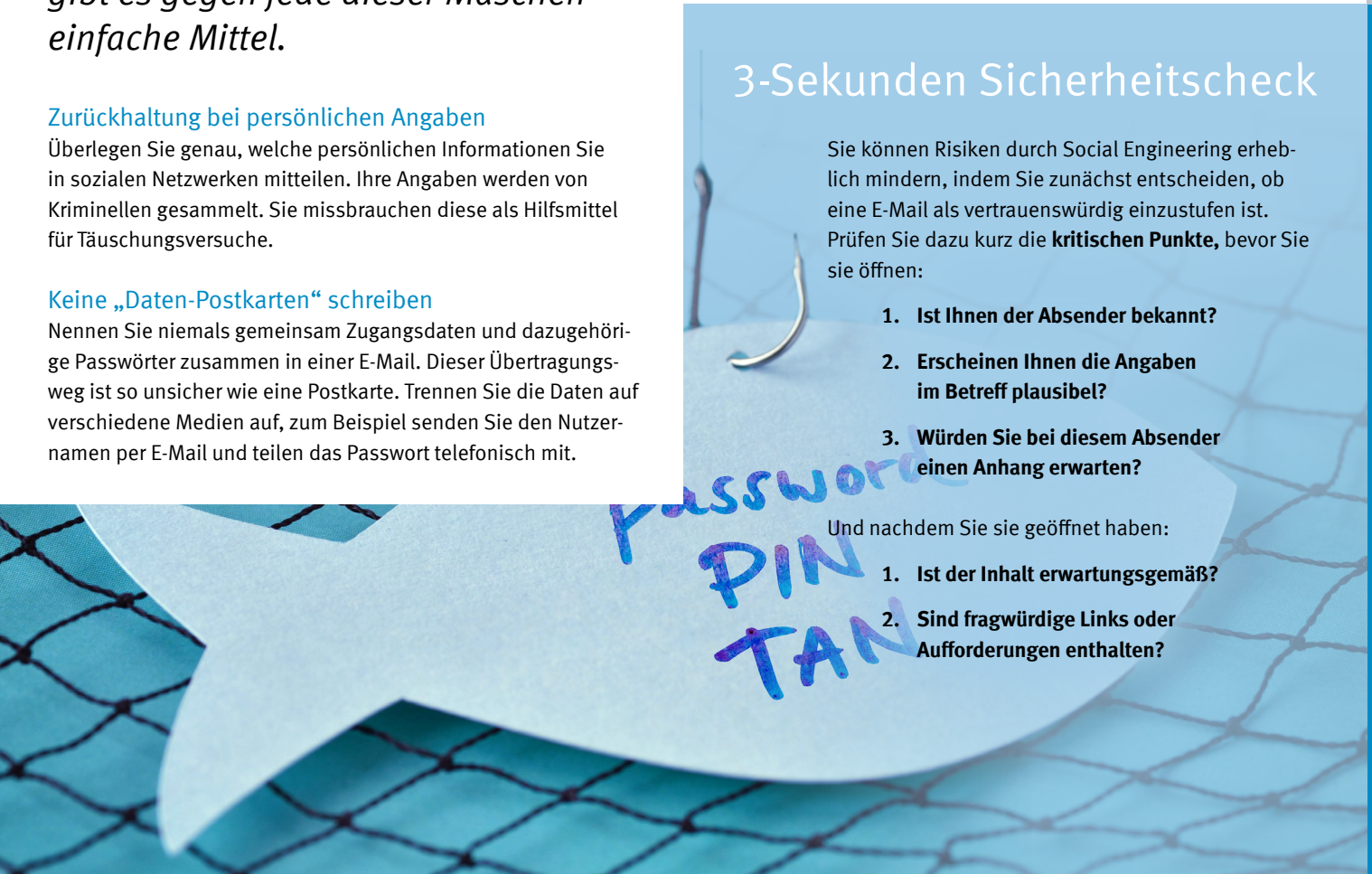
Geben Sie nie vertrauliche Informationen über Ihren Arbeitgeber und Ihre Arbeiten und Projekte preis, weder in privaten, noch in beruflichen sozialen Netzwerken oder Chatgruppen.

Vorsicht bei unbekannten Absendern

Sollte Sie auch nur ansatzweise das Gefühl haben, dass es sich bei der E-Mail über einen Angriffsversuch handeln könnte: Einfach nicht reagieren. (Noch besser: Löschen Sie die E-Mail und lassen Sie es dabei bewenden.)

Im Zweifel anrufen

Sollte eine Reaktion auf eine fragwürdige E-Mail zwingend erforderlich sein, vergewissern Sie sich durch einen Anruf beim Absender, dass es sich wirklich um *seine* E-Mail handelt.



3-Sekunden Sicherheitscheck

Sie können Risiken durch Social Engineering erheblich mindern, indem Sie zunächst entscheiden, ob eine E-Mail als vertrauenswürdig einzustufen ist. Prüfen Sie dazu kurz die **kritischen Punkte,** bevor Sie sie öffnen:

1. **Ist Ihnen der Absender bekannt?**
2. **Erscheinen Ihnen die Angaben im Betreff plausibel?**
3. **Würden Sie bei diesem Absender einen Anhang erwarten?**

Und nachdem Sie sie geöffnet haben:

1. **Ist der Inhalt erwartungsgemäß?**
2. **Sind fragwürdige Links oder Aufforderungen enthalten?**

Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:

Dienststelle:

Telefon:

E-Mail: