Köder erkennen und Betrug stoppen

So überlisten Sie Online-Betrüger:innen

Wenn Sie die Taktiken kennen, mit denen Kriminelle uns dazu bringen wollen, eine bestimmte Aktion auszuführen, beispielsweise auf einen Link in einer E-Mail zu klicken, können Sie potenzielle Betrugsversuche leichter erkennen. Online-Betrug wird zwar immer vielfältiger und zielt auf Einzelpersonen in verschiedenen Bereichen und Situationen ab, doch die von Kriminellen verwendeten Überzeugungsmethoden bleiben dieselben. Wenn Sie die verwendeten Techniken erkennen, können Sie sich selbst und Ihre Organisation online und offline besser schützen.

Wie funktioniert es?

Jeden Tag prasseln unzählige Marketingbotschaften auf uns ein – ob Fernsehwerbung oder Pop-up-Anzeigen im Netz –, alle mit dem Ziel, uns zu überzeugen und unser Verhalten zu beeinflussen.

Entscheidungen – etwa welche Produkte wir kaufen – erfordern kognitive Anstrengung. Um die Denkarbeit zu erleichtern, greift unser Gehirn automatisch auf mentale Abkürzungen zurück, die unser Handeln in vielen Situationen steuern. Genau diese Abkürzungen sind bekannt – und werden gezielt von denen ausgenutzt, die unser Verhalten beeinflussen wollen

Auch Kriminelle setzen solche Überzeugungstechniken ein – etwa um uns zum Klicken auf einen Link zu bewegen und dabei vertrauliche Daten abzugreifen. Diese Methoden, bekannt als Social Engineering, beruhen auf Täuschung und psychologischer Manipulation, die sich die Art und Weise zunutze machen, wie Menschen interagieren.

Anzeichen erkennen

Betrugsmaschen, die Sie dazu verleiten sollen, wertvolle Daten preiszugeben, nutzen oft eine oder mehrere der folgenden Techniken:

- **Autorität:** Gibt die Nachricht vor, von einer offiziellen Person zu stammen, beispielsweise von Ihrem CEO oder Ihrer Bank? Kriminelle geben sich oft als wichtige Personen oder Organisationen aus, um Sie unter Druck zu setzen, das zu tun, was sie wollen.

- **Dringlichkeit:** Werden Sie zu schnellem Handeln gedrängt, beispielsweise aufgrund eines zeitlich begrenzten Angebots oder eines Notfalls? Betrüger erzeugen ein Gefühl der Dringlichkeit, um Sie daran zu hindern, klar zu denken, und Sie zu schnellen Entscheidungen zu drängen.

- **Knappheit:** Wird Ihnen etwas angeboten, das nur begrenzt verfügbar ist, wie Konzertkarten, Geld oder bahnbrechende Therapien? Angst zu schüren, eine gute Gelegenheit zu verpassen, ist eine Technik, die Sie dazu bringen soll, schnell zu handeln.

- **Konsistenz:** Haben Sie jemals auf eine einfache E-Mail wie „Haben Sie kurs Zeit?“ geantwortet und wurden später um dringende Hilfe oder einen Gefallen gebeten? Wenn wir einmal zu etwas Kleinem zugestimmt haben, neigen wir dazu, konsistent zu bleiben und auch grösseren Bitten nachzukommen. Betrüger nutzen dies aus, um Sie Schritt für Schritt dazu zu bringen, Ja zu sagen.

- **Sympathie:** Wirkt Ihnen die Person die sie kontaktiert vertraut – vielleicht weil sie freundlich auftritt, ähnliche Interessen zeigt oder Sie an jemanden erinnert, den Sie kennen? Social Engineers nutzen genau diesen Effekt: Wir vertrauen eher Menschen, die uns sympathisch erscheinen, als solchen, die uns unsympathisch sind.

- **Gegenseitigkeit:** Hat Ihnen jemand einen kleinen Gefallen getan, Ihnen beispielsweise einen Rat gegeben oder Hilfe angeboten, bevor er Sie um etwas gebeten hat? Diese Technik nutzt Ihre natürliche Neigung, einen Gefallen zu erwidern, auch wenn dies in diesem Falle nicht in Ihrem Interesse ist.

Was können Sie tun?

Betrüger nutzen psychologische Tricks, um Ihr Verhalten zu beeinflussen. Wenn Sie sich dieser Taktiken bewusst sind, können Sie Ihre eigenen Reaktionen besser verstehen und Betrugsversuche leichter erkennen und vermeiden.

Tipps: Betrug erkennen und vermeiden

- Nehmen Sie sich Zeit, um Anzeichen für möglichen Betrug zu erkennen.
- Fühlen Sie sich nicht unter Druck gesetzt, schnell zu reagieren. Überlegen Sie, bevor Sie handeln. Machen Sie eine Pause, prüfen Sie die Plausibilität der Anfrage und führen Sie die unten beschriebenen Echtheitsprüfungen durch.
- Überprüfen Sie die Echtheit eines Anrufs oder einer Nachricht. Wenden Sie sich direkt an die Organisation oder Person, die den Anruf oder die Nachricht angeblich gesendet hat, und verwenden Sie dazu die Angaben auf der offiziellen Website. Antworten Sie nicht auf die Adresse oder Nummer in der Nachricht.
- Geben Sie keine persönlichen Daten oder Bankdaten in einer E-Mail weiter. Denken Sie daran, dass Banken und andere offizielle Stellen Sie niemals danach fragen werden.

Be mindful. Stay safe.

Machen Sie sich mit den Techniken vertraut, mit denen Kriminelle versuchen, Vertrauen zu erschleichen und Sie zu betrügen. Wenn Ihnen etwas seltsam vorkommt oder zu gut, um wahr zu sein, ist es das wahrscheinlich auch.

Gehen Sie auf wichtige Anfragen nur dann ein, wenn Sie Ruhe haben und sich voll darauf konzentrieren können – nicht unterwegs auf kleinem Screen oder zwischen Tür und Angel. Und wenn Ihnen etwas verdächtig vorkommt: Fragen Sie nach und prüfen Sie die Echtheit. Das gibt Ihnen Sicherheit.

Erfahren Sie mehr

🔗 Phishing: Spot and report scam emails, texts, websites and calls (source: NCSC UK)
🔗 Psychology of the Phish: Leveraging the Seven Principles of Influence (source: NCC Group)