SOPHOS

Security made simple.

Zehn verräterische Hinweise auf Phishing

Phishing-E-Mails können alle möglichen Formen annehmen und vom Umfang her sehr unterschiedlich sein, aber zum Glück gibt es Hinweise, auf die Sie achten können, um potenziellen Scam zu erkennen.

1. **Irgendetwas stimmt einfach nicht.** Kommt Ihnen an den E-Mails irgendetwas komisch vor? Klingen sie zu gut, um wahr zu sein? Vertrauen Sie Ihrem Instinkt, wenn er Ihnen zur Vorsicht rät.

2. **Allgemeine Anreden.** Anstatt Sie direkt anzusprechen, werden in Phishing-E-Mails häufig allgemeine Anreden wie „Sehr geehrter Kunde" verwendet. Die Verwendung unpersönlicher Anreden spart den Cyberkriminellen Zeit, so dass sie die Anzahl der potenziellen Opfer maximieren können.

3. **Links zu offiziell erscheinenden Websites, auf denen Sie aufgefordert werden, sensible Daten einzugeben.** Diese gefälschten Websites sind oftmals sehr überzeugend, daher sollten Sie vor der Eingabe persönlicher oder vertraulicher Daten genau prüfen, ob die Website wirklich echt ist.

4. **Unaufgefordert zugesendete E-Mails mit spezifischen Informationen zu Ihrer Person.** Daten wie Berufsbezeichnung, frühere Arbeitgeber oder persönliche Interessen können auf Social-Networking-Websites wie LinkedIn in Erfahrung gebracht und dann verwendet werden, um eine Phishing-E-Mail überzeugender wirken zu lassen.

5. **Einschüchternde Formulierungen.** Phishing-Angreifer verwenden oftmals Formulierungen, die Ihnen Angst machen sollen (wie z. B. dass Ihr Konto manipuliert wurde). Damit sollen Sie dazu gebracht werden, etwas zu tun, ohne darüber nachzudenken, und dabei Informationen preisgeben, die Sie normalerweise nie weitergeben würden.

6. **Grammatik- oder Rechtschreibfehler.** Fehler sind oft ein eindeutiger Hinweis auf Phishing. Auch ein ungewöhnlicher Satzbau sollte bei Ihnen die Alarmglocken läuten lassen.

7. **Angebliche Dringlichkeit.** Zum Beispiel: „Wenn Sie nicht innerhalb von 48 Stunden antworten, wird Ihr Account gesperrt." Ihnen wird vorgegaukelt, dass die Uhr tickt, und die Angreifer hoffen, dass Sie darauf anspringen.

8. **„Sie sind der Hauptgewinner!"** Solche Phishing-E-Mails sind weit verbreitet, aber leicht zu erkennen. Eine ähnliche, noch raffiniertere Variante ist, dass Sie zur Teilnahme an einer Umfrage eingeladen werden (bei der Sie persönliche Daten preisgeben) und dafür ein kleines Dankeschön erhalten.

9. **„Verifizieren Sie Ihren Account."** Diese E-Mails imitieren echte E-Mails und bitten Sie, Ihr Konto auf einer Website oder bei einem Unternehmen zu verifizieren. Stellen Sie sich immer die Frage, warum Sie zur Verifizierung aufgefordert werden. Es ist sehr wahrscheinlich, dass es sich um Scam handelt.

10. **Cybersquatting.** Oftmals registrieren Cyberkriminelle Website-Namen, die Ähnlichkeit mit einer offiziellen Website haben, und „besetzen" diese (Squatting), in der Hoffnung, dass die Benutzer auf die falsche Seite gehen, wie z. B. www.g00gle.com statt www.google.com. Nehmen Sie sich immer einen Moment Zeit, um die URL zu prüfen, bevor Sie Ihre persönlichen Daten eingeben.

Weitere Informationen und Tools zum Schutz vor Phishing finden Sie auf www.sophos.de/phishing.