

Phishing - So schützen Sie sich

Bei Phishing-Angriffen versuchen Kriminelle, meist über perfekt gefälschte Mails und Webseiten an die Passwörter oder Bankdaten der Anwender zu gelangen. Die User geben demnach ihre Informationen selbst preis. Um darauf nochmals aufmerksam zu machen, spendiert Yahoo zehn Sicherheitstipps:

1. **Gesundes Misstrauen** - Eine grundsätzliche Skepsis gegenüber Webseiten, die dazu auffordern, eine ID oder ein Passwort einzugeben, ist das oberste Gebot. Vor allem sollte man keine Login-Daten auf Seiten eingeben, die man per E-Mail oder Messenger erhalten hat. Die gängigste Methode, an fremde Daten zu gelangen, ist es, Homepages nachzubauen. Tipp: Webseiten mit sensiblen Inhalten wie Onlinebanking oder E-Mail sollten grundsätzlich über die Bookmark-Sammlung oder Suchmaschinen aufgerufen werden.
2. **Alarmsignal fehlerhafte URL** - Denn daran sind Phishing-Webseiten oft noch gut zu erkennen. Meist verstecken sich in den Adressen Rechtschreibfehler oder zusätzliche Wörter wie beispielsweise www.yahOOO.com oder www.yahoo-members.com. Oft findet man auch Tippfehler oder veraltete Inhalte. Grundsätzlich ist es ratsam, sich direkt über die Startseite einzuloggen.
3. **Schutz durch Anmeldesiegel** - Zusätzlichen Schutz vor Passwortklau gewährleistet ein sogenanntes Anmeldesiegel. Dabei handelt es sich um eine geheime persönliche Nachricht oder ein Foto, das vom Nutzer eingerichtet wurde und beim Login angezeigt wird. So können Nutzer sicherstellen, dass sie sich auf der richtigen Webseite befinden. Fehlt das Siegel oder sieht es anders aus, etwa durch veränderte Farben, ist man unter Umständen auf einer Phishing-Seite.
4. **Zugangsdaten unter Verschluss** - Ein Passwort darf niemals per E-Mail versendet werden. Ein seriöses Unternehmen fragt nie nach dem Passwort - weder per E-Mail noch telefonisch. Wer eine solche Anfrage erhält, sollte davon ausgehen, dass es sich um Betrug handelt und auf keinen Fall darauf reagieren.
5. **Achtung Pop-Up-Warnung** - Pop-up-Warnungen immer sorgfältig lesen, aber nicht anklicken. Des Öfteren tauchen beim Surfen im Internet Pop-up-Fenster auf, die Nutzer z. B. dazu auffordern, eine Software zu installieren, die das Betriebssystem angeblich sicherer macht. Solche Hinweise sind meistens betrügerisch, sodass man sich auf diese Weise fehlerhafte Software oder Viren auf seinen PC lädt.
6. **Trügerische Lotterie-E-Mails** - Oft landen E-Mails eines gefälschten Lotterie-Gewinnspiels im Namen von bekannten Unternehmen im Posteingang mit der vermeintlich frohen Botschaft, man hätte viel Geld gewonnen und müsse jetzt nur seine Kontodaten angeben. Yahoo beispielsweise betreibt keine Lotterie, und diese E-Mails sind immer betrügerisch. Nachrichten mit dem Absender «xxx Lottery» sollten deshalb ungelesen in den Papierkorb wandern und vorher als «Spam» gemeldet werden.
7. **Richtiges Passwort** - Bei der Passwortwahl sollte man darauf achten, dass man es sich gut merken kann, es andere aber nicht erraten können - wie es beispielsweise beim Geburtsdatum leicht der Fall ist. Es sollte möglichst lang sein (mindestens 6 Zeichen) und im Idealfall aus einer Kombination aus Buchstaben, Zahlen und Standardsymbolen bestehen. Wichtig ist auch die Gross- und Kleinschreibung. Variiert man, wird es für Fremde schwieriger, das Passwort zu knacken. Eine gute Taktik ist, einen Spruch oder eine Zeile aus dem Lieblingslied als Passwort zu verschlüsseln.
8. **Passwort-Wechsel** - Passwörter sollten regelmässig ausgetauscht werden. Das erschwert Zugriffe von Fremden zusätzlich. Ausserdem empfiehlt es sich, für verschiedene Webseiten und Portale unterschiedliche Passwörter einzusetzen.
9. **Aktuelle Antiviren-Software** - Antiviren-Software sollte nicht nur auf dem Rechner installiert sein, sondern auch regelmässig aktualisiert werden. Nur dann ist ein optimaler Schutz gewährleistet, denn täglich kursieren neue Viren, Würmer & Co. im Netz. Wenn es der genutzte Service anbietet, empfiehlt es sich, ein «automatisches Update» einzustellen. Darüber hinaus sollte man auch Browser- oder Applikationen-Software, wie beispielsweise die des Messengers, immer aktuell halten.
10. **Hilfe und Rat suchen** - Bestehen Unklarheiten oder der Verdacht, eines Betrugs, dann sollte sofort das angebliche Unternehmen kontaktiert werden. Denn nur durch gute Zusammenarbeit, Austausch und Kenntnis aller Risiken kann der Schutz persönlicher Daten gewährleistet werden.