Phishing-Analyse:

Gefälschte Microsoft 365-Anmeldeaufforderung

Inhalt

Übersicht

Das Phishing-Beispiel

Erkennungsmerkmale und Warnsignale

Potenzielle Schäden

Korrektes Verhalten

Übersicht

Angriffsart: Credential Phishing (Erbeuten von Zugangsdaten)

Schwierigkeitsgrad: Mittelstufe

Risikopotenzial: Hoch (ermöglicht Zugriff auf Unternehmensdaten und kann zu weiteren Angriffen führen)

Zielgruppe: Alle Mitarbeiter

Das Phishing-Beispiel

Von: **Microsoft** <microsoft-365-noreply@ms-secure-login.com>

An: [Empfänger]

Betreff: **Wichtig: Ihre Microsoft 365-Anmeldung ist abgelaufen**

Sehr geehrter Benutzer,

Wir stellen fest, dass Ihre Microsoft 365-Anmeldung abgelaufen ist. Um Datenverlust zu vermeiden und weiterhin auf Ihre E-Mails und Dokumente zugreifen zu können, müssen Sie Ihre Anmeldeinformationen innerhalb von 24 Stunden aktualisieren.

[Jetzt anmelden und aktualisieren]

Falls Sie nicht innerhalb von 24 Stunden reagieren, wird Ihr Konto für Sicherheitszwecke gesperrt und alle gespeicherten Daten werden möglicherweise nicht wiederherstellbar sein.

Mit freundlichen Grüßen

Das Microsoft 365-Team

Diese Nachricht wurde automatisch generiert. Bitte antworten Sie nicht auf diese E-Mail.

Erkennungsmerkmale und Warnsignale

1. Absenderadresse

Verdächtig: microsoft-365-noreply@ms-secure-login.com

Korrekt wäre: Absender-Domains enden bei Microsoft stets mit microsoft.com oder outlook.com

2. Betreffzeile

Warnsignal: Verwendung von Dringlichkeitsformulierungen ("Wichtig", "abgelaufen")

Taktik: Erzeugen von Zeitdruck und Sorge um Datenverlust