NACHRICHTEN AG

26. August 2024

Vorsicht: Betrügerische E-Mails der Steuerverwaltung im Umlauf!

Achtung: Aktuell kursieren gefälschte E-Mails der Steuerverwaltung in M-V. Informieren Sie sich über die Risiken und Vorgehensweisen.

In letzter Zeit sind zahlreiche Bürger in Mecklenburg-Vorpommern Ziel von Phishing-Emails geworden, die sich als Mitteilungen der Steuerverwaltung ausgeben. Diese Mails und Nachrichten, die oft mit Namen wie ELSTER oder Finanzamt abgesendet werden, versuchen, die Empfänger dazu zu bringen, sensible Informationen preiszugeben oder Anhänge zu öffnen, die letztlich als gefährlich eingestuft werden. Betrüger nutzen diesen Trick, um ungerechtfertigte Steuererstattungen zu erlangen, was die Bedeutung der Aufklärung über solche Maschen verdeutlicht.

Die Steuerverwaltung betont explizit, dass sie niemals persönliche Daten wie Steuernummern, Bankverbindungen oder die PINs von Kreditkarten per E-Mail anfordert. Dies ist entscheidend zu wissen, um nicht auf die manipulativen Taktiken der Täter hereinzufallen. Nutzer sind gut beraten, solche Nachrichten sofort zu löschen, um mögliche Schaden zu vermeiden.

Details zu den Betrügereien

Phishing, ein Begriff, der von “Fishing” (Fischen) abgeleitet ist, bezieht sich auf Methoden, bei denen Betrüger versuchen, wertvolle Informationen von Nutzern zu „fischen“. Die aktuelle Reihe von Emails wird in einem formellen, aber bedrohlich

anmutenden Ton verfasst. Es wird behauptet, dass der Empfänger ein Dokument zur Steuererstattung öffnen muss, um angebliche Rückzahlungen zu erhalten. In Wirklichkeit ist der Anhang oft voller Malware, also schadhafter Software, die darauf abzielt, die Kontrolle über das Gerät des Nutzers zu erlangen oder weiteren Datenklau zu ermöglichen.

Die auf diese Weise betrügerisch erlangten Daten können dann für Identitätsdiebstahl oder andere Formen finanzieller Betrügereien genutzt werden, was einem enormen Risiko für die Betroffenen gleichkommt. Bayern und andere Bundesländer haben ähnliche Vorfälle bestätigt, was deutlich macht, dass dies ein bundesweiter Trend ist, der ein starkes Sicherheitsbewusstsein erfordert.

Wichtige Präventionsmaßnahmen

Bürger werden ermutigt, sich über die unterschiedlichen Arten von Phishing zu informieren, um besser in der Lage zu sein, solche Emails zu erkennen. Einige Anzeichen für Phishing-Mails sind:

- Unbehagliche oder ungewöhnliche Absenderadressen
- Rechtschreibfehler oder unprofessionelles Design der Email
- Dringliche Aufforderungen zur Preisgabe von Daten

Die fortlaufende Aufklärung über diese Bedrohungen ist entscheidend. Die Steuerverwaltung von Mecklenburg-Vorpommern fordert daher die Bürger auf, wachsam zu bleiben und verdächtige Nachrichten, die sie erhalten, zu melden. Eine enge Zusammenarbeit mit den IT-Abteilungen und Cyber-Sicherheitsexperten ist unerlässlich, um die Integrität und Sicherheit der digitalen Kommunikation zu gewährleisten.

Um die Öffentlichkeit besser zu informieren, bieten viele offizielle Stellen Schulungen und Ressourcen an, die erklären, wie man mit Online-Bedrohungen umgeht, und wie man seine

persönlichen Daten schützt. Das Wissen über Cyber-Sicherheit wird zunehmend zu einer notwendigen Fähigkeit in unserer digitalisierten Welt.

Die Auswirkungen dieser Phishing-Welle können mmomentan nur schwer zu bemessen sein, aber sie verdeutlicht das wachsende Problem der Internetkriminalität. Umso wichtiger ist es, dass jeder für sich selbst Verantwortung übernimmt und über die Methoden und Mittel, die Kriminelle verwenden, informiert bleibt.

Wachsamkeit ist der Schlüssel

In einer Zeit, in der digitale Kommunikation eine der Hauptformen des Informationsaustauschs ist, ist es von enormer Bedeutung, sich der Gefahren, die im Internet lauern, bewusst zu sein. Mit zunehmender Digitalisierung ist nicht nur die Technik, sondern auch die Sensibilisierung für solche Themen unerlässlich.

Die Steuerverwaltung und andere Institutionen setzen weiterhin auf Aufklärung und Prävention, damit Bürger sich sicherer bewegen können im digitalen Raum. Daher ist es wichtig, sich laufend zu informieren und die eigene digitale Hygiene zu wahren.

Erhöhte Sicherheitsmaßnahmen zur Bekämpfung von Phishing

In Anbetracht der zunehmenden Phishing-Angriffe haben viele Steuerverwaltungen, sowohl in Deutschland als auch international, ihre Sicherheitsprotokolle verbessert. Die Verwendung von Zwei-Faktor-Authentifizierung (2FA) ist mittlerweile weit verbreitet, um den Zugriff auf Steuerportale sicherer zu machen. Diese Maßnahme erfordert, dass die Nutzer neben ihrem Passwort einen zusätzlichen Sicherheitscode verwenden, der oft per SMS an ihre registrierte Handynummer

gesendet wird.

Viele Behörden betonen auch die Bedeutung von Aufklärungskampagnen, um Bürger über die Gefahren von Phishing aufzuklären. Diese Kampagnen informieren die Öffentlichkeit über die häufigsten Merkmale von Phishing-E-Mails und rufen dazu auf, verdächtige Nachrichten zu melden. In Deutschland läuft beispielsweise eine Initiative, die über die Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zugänglich ist.

Wie erkennt man Phishing-Mails?

Einige grundlegende Merkmale können helfen, Phishing-E-Mails zu identifizieren. Oft erscheinen die Absenderadressen nicht authentisch und enthalten beispielsweise zusätzliche Buchstaben oder Domainnamen, die nicht der offiziellen Seite entsprechen. Außerdem verwenden Phishing-Nachrichten häufig eine drängende Sprache, um den Empfänger zur schnellen Handlung zu bewegen.

Die Steuerverwaltung rät, immer vorsichtig zu sein, wenn in E-Mails persönliche Informationen angefordert werden. Bürger sollten stattdessen direkt die offizielle Webseite der Steuerbehörde besuchen oder telefonisch Kontakt aufnehmen, um Informationen zu verifizieren.

Rechtliche Maßnahmen gegen Phishing

Die Bekämpfung von Phishing ist nicht nur eine Frage der IT-Sicherheit, sondern auch der rechtlichen Durchsetzung. Strafverfolgungsbehörden weltweit arbeiten zusammen, um cyberkriminelle Netzwerke zu identifizieren und rechtlich gegen diese vorzugehen. In Deutschland verfolgt das Bundeskriminalamt (BKA) gezielt Fälle von Online-Betrug und richtet spezielle Einheiten zur Cyberkriminalität ein.

Darüber hinaus gibt es zahlreiche internationale Abkommen, die

den Austausch von Informationen und die Zusammenarbeit zwischen den Ländern fördern, um Cyber-Kriminalität effektiv zu bekämpfen. Die europäische Polizeibehörde Europol setzt sich ebenfalls für eine verstärkte Zusammenarbeit in europäweiten Ermittlungsteams ein.

Statistiken zu Phishing-Angriffen

Die Zunahme von Phishing-Angriffen wird durch aktuelle Statistiken untermauert. Laut einer Studie des Branchenverbands Bitkom haben rund 80 % der Unternehmen in Deutschland im Jahr 2022 Phishing-Angriffe erlebt. Darüber hinaus sind 30 % der Betroffenen sogar auf einen solchen Angriff hereingefallen. Diese Zahlen verdeutlichen die Dringlichkeit von Sensibilisierungsmaßnahmen und die Notwendigkeit für Verbesserungen in der Sicherheitsinfrastruktur. Für Einzelpersonen kann derartige Aufklärung entscheidend sein, um sich vor identitätskriminellen Aktivitäten zu schützen.

Die zunehmende Bedrohung durch Phishing-Angriffe stellt somit nicht nur ein Risiko für Einzelpersonen dar, sondern auch für Unternehmen und Regierungsbehörden, die regelmäßig mit sensiblen Daten arbeiten.

Details