- **Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.**

Spam-Welle wegen angeblicher Finanzamtsrückzahlung – ACHTUNG: Phishing-Seite

Art der Bedrohung

Durch die Eingabe Ihrer Kreditkartendaten inkl. des CVV-Codes und des 3D Secure Passwortes erlangen die Täter volle Kontrolle über diese und können Abbuchungen bis zum Limit der Karte durchführen; schwerer finanzieller Schaden droht!

Modus Operandi

Aktuell langen in der Meldestelle des C4 zahlreiche Mitteilungen über den Erhalt einer E-Mail, welche vorgibt vom Bundesministerium für Finanzen zu sein, ein. Die Mail-Absenderadresse verweist auch tatsächlich auf bmf@bmf.gv.at, allerdings ist der Empfänger als Adressat nicht persönlich angeführt, sondern weist die Bezeichnung „Recipients“ auf eine Massenaussendung hin.

Die E-Mail selbst macht einen professionellen, nicht aufdringlichen Eindruck, auffällig ist jedoch wieder einmal eine etwas schlechte Übersetzung und damit zusammenhängende Fehler in der Wortwahl und Satzstellung.

Inhalt der E-Mail ist eine angebliche Steuergutschrift in der Höhe von € 716,43, welche über ein Web-Formular beantragt werden kann. Wird der Weblink tatsächlich aufgerufen, gelangt man auf eine Webseite welche der tatsächlichen gut nachgebaut ist. Es erscheint direkt ein Formular, welches zur Eingabe von Kreditkartendaten auffordert.

Werden hier tatsächlich echte Daten eingegeben, erlangen die Täter volle Kontrolle über die Kreditkarte und können somit schweren finanziellen Schaden zufügen. Zudem kann nicht ausgeschlossen werden, dass auf derartigen Webseiten nicht zudem eine Infektion des Computersystems mit Schadsoftware, aktuell handelt es sich zumeist um Ransomware, erfolgt.

Ransomware ist derzeit in verschiedensten Versionen tagtäglich dafür verantwortlich, dass sowohl im privaten als auch im Firmenbereich die Daten von Computer- und Netzwerksystemen verschlüsselt und eine Entschlüsselung nur nach Bezahlung einer erpressten Summe mittels BitCoin möglich ist.

Empfohlene Vorgangsweisen:

- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen oder wenn Sie keine entsprechenden Mitteilungen erwarten.
- Kontrollieren Sie nach Möglichkeit die tatsächliche Absenderadresse, achten Sie auf Ungereimtheiten. Bei angeführten Weblinks legen Sie den Mauszeiger über den entsprechenden Link, ohne diesen zu aktivieren. Sollte die Web-Link-Adresse aufscheinen, kontrollieren Sie, ob diese tatsächlich zum Absender gehört.
- Achten Sie auf die Schreibweise und Rechtschreibung solcher Nachrichten, Täter verwenden hier gerne Übersetzungsprogramme, wodurch der Betrug leicht erkennbar ist.
- Geben Sie online niemals Ihre Bank- oder Kreditkartendaten über Aufforderung bekannt, sofern es sich nicht gerade um die Abwicklung eines Geschäftes (online-Kauf) handelt.
- Seien Sie bei der Bekanntgabe Ihrer persönlichen Daten vorsichtig, geben Sie niemals mehr als notwendig bekannt, übermitteln Sie keine Ausweiskopien. All diese Daten könnten für den Ursprung des nächsten Betruges zur Verwendung kommen.
- Öffnen Sie keinesfalls Ihnen unbekannte Dateianhänge, ohne sich vorher von deren „Echtheit“ zu überzeugen. Werden Ihnen Bewerbungsunterlagen, Paketverständigungen udgl. zum Download „angeboten“, tun Sie dies bitte nicht! Wenn Sie dennoch der Ansicht sind, dass es sich um echte und notwendige Dokumente handelt, laden Sie die Datei nur in einer gesicherten Umgebung (Sandbox) und auf nicht produktiven Geräten herunter und öffnen diese dann auch dort.
- Wenn Sie sich unsicher sind, öffnen Sie derartige Dateien in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) oder bedienen Sie sich unterstützender Seiten im Internet (z.B. Virustotal.com).
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: http://www.bmi.gv.at.

Text und Grafik der E-Mail:

Sehr geehrte Damen und Herren, diese Nachricht war heute zweimal in meinem Postfach:

Gesendet: Donnerstag, 13. Oktober 2016 um 05:10 Uhr
Von: "bmf.gv.at"
An: Recipients
Betreff: Benachrichtigung bei Rückkehr.

BMF
BUNDESMINISTERIUM FÜR FINANZEN

Lieber Steuerzahler BMF-Bundesministerium,

Wir haben einen Fehler in der Berechnung der Steuer der letzten Zahlung in Höhe.

Von 716,43 Euro identifiziert. Um die Überzahlung zurückkehren.

Müssen wir noch einige weitere Details, wonach die Mittel werden auf Ihr Bankkonto,

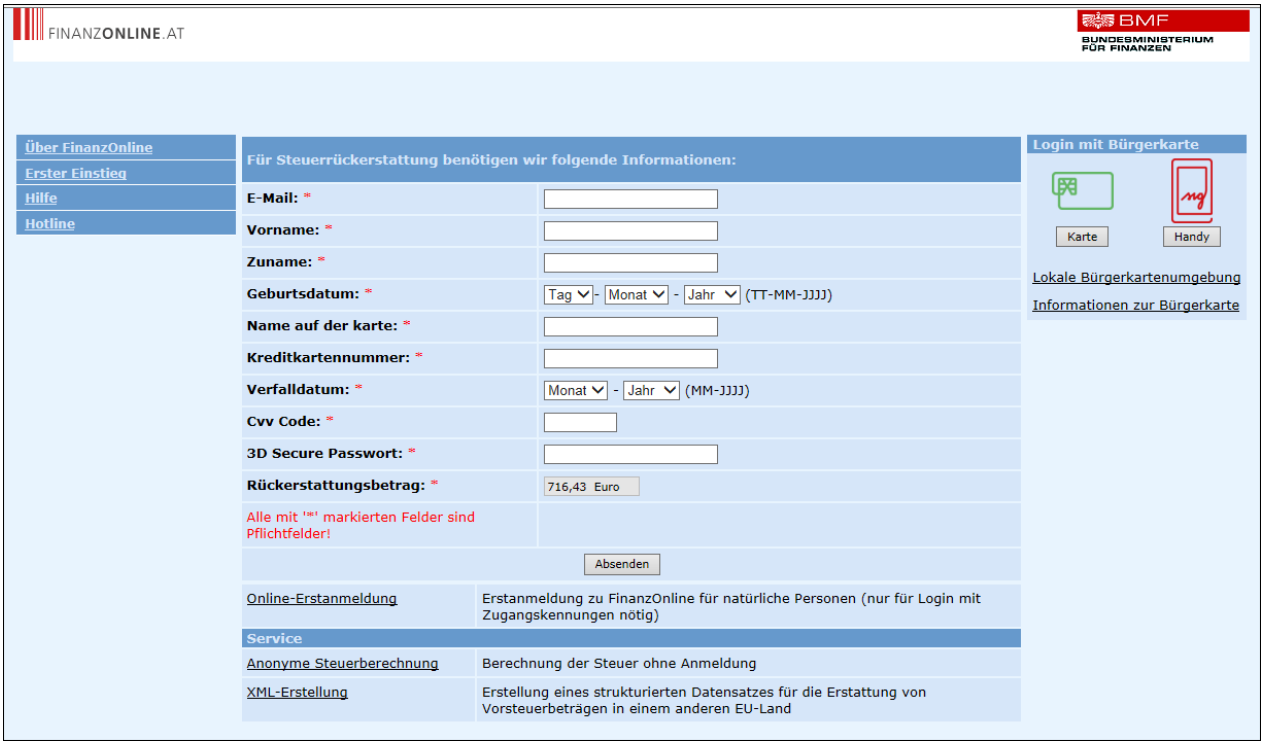
Gutgeschrieben bestätigen.

Füllen Sie bitte das Steuer formular im Anhang zu dieser E-Mail und ermöglichen es uns 3-5 Werktage, um es zu verarbeiten.

Referenz-Nummer: 45520-831-F972-C10

Copyright © 2016 Bundesministerium für Finanzen

Grafische Darstellung der Phishing-Seite:



Weiterführende und erklärende Links:

Wikipedia – Phishing: was ist Phishing (https://de.wikipedia.org/wiki/Phishing)

Wikipedia – Ransomware: was ist Ransomware (https://de.wikipedia.org/wiki/Ransomware)

Watchlist-Internet –

- So können Sie sich vor Phishing schützen (https://www.watchlist-internet.at/phishing/so-koennen-sie-sich-vor-phishing-schuetzen/)
- Wenn Sie in die Phishing-Falle getappt sind (https://www.watchlist-internet.at/phishing/wenn-sie-in-die-phishing-falle-getappt-sind/)

Bundeskriminalamt – Betrugsformen im Internet: (http://www.bmi.gv.at/cms/BK/betrug/start.aspx)

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG

Hinweis: Die vorliegende Information beruht auf einer Momentaufnahme aus dem Geschehen in der C4-Meldestelle ohne Berücksichtigung allen Falls vorhandener statistischer Daten aus dem Bundesgebiet und dient einem eingeschränkten Empfängerkreis zu Informations- und Präventionszwecken. Der beschriebene Tathergang sowie dazugehörige technische Details wurden im Rahmen der hier vorhandenen Möglichkeiten recherchiert und erheben keinen Anspruch auf Vollständigkeit. Angeführte Web-Links zu weiterführenden Artikeln und Informationen wurden zwar bei der Erstellung des Newsletters auf ihre sachliche und inhaltliche Richtigkeit überprüft, es besteht jedoch keine Haftbarkeit für das .BK bei Änderung dieser Inhalte durch Dritte. Medienanfragen sind ausschließlich an die Pressestelle des Bundeskriminalamts zu stellen.