Merkblatt zur Mitarbeiterbelehrung e-loading-Betrug mit Arbeitsanweisung

Bitte beachten Sie folgenden Hinweis:

Dieses Merkblatt enthält nur erste Hinweise und erhebt keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

Das beigefügte Muster ist, wie alle Muster, den individuellen Gegebenheiten entsprechend anzupassen und stellt lediglich eine grundsätzliche Vorlage dar. Haftung für Anpassungen des Musters und ihre Folgen können wir nicht übernehmen.

Das Muster ersetzt nicht die persönliche Beratung durch Ihren Verband, Rechtsanwalt oder Steuerberater.

Generell sind in diesem Formular die offengelassenen freien Stellen jeweils nach den individuellen Bedürfnissen zu ergänzen.

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit verwenden wir die männliche Form (generisches Maskulinum), z. B. „der Mitarbeiter“. Wir meinen immer alle Geschlechter im Sinne der Gleichbehandlung. Die verkürzte Sprachform hat redaktionelle Gründe und ist wertfrei.

Bei Fragen wenden Sie sich an den FTG e.V. unter der Telefonnummer: 0228-917230.

Mitarbeiterbelehrung und Arbeitsanweisung zum e-loading-Betrug

Betrugsversuche am Telefon:

Die verwendete Masche ist fast immer identisch. Die Betrüger melden sich telefonisch, meist zu Zeiten, in denen vermutet wird, dass die Stationsleitung nicht vor Ort und auf der Station wenig Personal vorhanden ist. Rückfragen des Angerufenen sind damit kaum möglich.

Die Anrufer stellen sich entweder als Mitarbeiter von Lieferanten oder des Kassenherstellers, teilweise sogar als Verwandte des Tankstellenbetreibers vor. Bitte beachten Sie, dass hier vielleicht auch noch andere Tricks versucht werden könnten. Meistens werden im Display auch die richtigen dazugehörigen Telefonnummern angezeigt. Diese sind jedoch stets manipuliert.

Immer beliebter wird auch die Masche, dass die Mobilfunknummer des Tankstellenunternehmers angezeigt wird, der angeblich gerade nicht selbst anrufen kann, aber unbedingt Cash-Codes braucht und deswegen seinen Sohn, Vater oder besten Freund mit seinem Handy anrufen lässt.

Der Anrufer wird dann behaupten, entweder ein Update durchführen zu müssen oder eine Störung beseitigen zu wollen. In der Regel wird daneben ein Druckszenario aufgebaut, warum dies jetzt unbedingt sofort gemacht werden muss (hoher drohender Schaden, große Eilbedürftigkeit, mit Stationsleitung so abgesprochen, usw.). Wenn das Personal die Codes nicht herausgeben möchte, werden noch härtere Konsequenzen angedroht: Das e-loading-Gerät werde monatelang nicht funktionieren, der Chef sehe einer Strafe wegen eines Verstoßes gegen den Jugendschutz entgegen usw.

Ist der Anrufer mit seinem Betrug erfolgreich, lässt er den Mitarbeiter mehrere Paysafecard- oder sonstige Voucher ausdrucken. Schließlich will der Anrufer die Cash-Codes telefonisch mitgeteilt bekommen.

Hier handelt es sich ausnahmslos um Betrugsversuche! Niemand, ist befugt oder ermächtigt, telefonisch nach einem Cash-Code zu fragen. Dies gilt unter allen Umständen!

Betrugsversuche in der Station:

Den bisherigen Höhepunkt bilden Fälle, in denen die Betrügereien nicht mehr am Telefon, sondern „persönlich“ durchgeführt werden: Der meistens gut gekleidete „Mitarbeiter“ von Lekkerland oder Transact oder eines sonstigen Lieferanten mit ebenso gut gefälschtem Firmenausweis macht sich persönlich die Mühe, in der Tankstelle vorbeizuschauen, um das Terminal zu überprüfen oder ein Update durchzuführen – und dabei natürlich Cash-Codes zu generieren.

Älter und bekannter ist ein anderer Trick, wenn die Codes bereits ausgehändigt worden waren, während der Zahlvorgang mit der (dann natürlich nicht funktionierenden Kreditkarte) noch andauerte. Die Betrüger fotografierten, während sie scheinbar telefonierten, die Codes mit ihrem Fotohandy ab.

Nachdem das Telefonieren wohl doch zu auffällig war, kommt dieser Trick jetzt offenbar in einer technisch verfeinerten Variante neu auf. Ein Kunde mit Brille - der Täter - betritt den Shop und möchte Paysafe-Codes kaufen. Der Mitarbeiter druckt diese aus und legt sie dem Kunden vor, bzw. legt sie sichtbar auf die Arbeitsfläche am Kassenplatz. Der Täter möchte mit EC- oder Kreditkarte bezahlen. Die Karten funktionieren aber nicht und der Täter verabschiedet sich. Was jedoch nicht bemerkt wurde, ist die Tatsache, dass die Brille des Täters eine eingebaute Mini-Kamera (CCTV) hatte. Mit dieser Brillen-Kamera wurden die Paysafe-Codes aufgenommen und schon wenige Minuten später vom Ausland aus eingelöst!

Arbeitsanweisung:

- **Geben Sie niemals einen PIN-Code ohne vorherige Bezahlung heraus** – egal, ob persönlich, telefonisch oder per Email. Dies gilt auch für einzelne Ziffern von PIN-Codes.
- Niemand außer Ihnen selbst darf in Ihrer Schicht an das Terminal.
- Lassen Sie sich nicht verunsichern.
- Erfragen Sie Namen und Telefonnummer des Anrufers.
- Beenden Sie das Telefonat und informieren Sie die Stationsleitung. Diese wird die Polizei in Kenntnis setzen.
- Können Sie die Stationsleitung nicht erreichen, rufen Sie selbst die Polizei unter 110 an.

Kenntnisnahme:

Mit meiner Unterschrift bestätige ich die Kenntnisnahme dieser Mitarbeiterbelehrung und verpflichte mich zur Einhaltung der darin enthaltenen Arbeitsanweisung.

Ich wurde vom Arbeitgeber ausführlich über die Möglichkeit aufgeklärt, dass Betrüger über das Telefon, per Mail oder persönlich in der Tankstelle versuchen, PIN-Nummern oder Cash-Codes zu erlangen. Mir ist bewusst, dass ich niemals und unter keinen Umständen Codes oder PIN-Nummern ohne vorherige Bezahlung herausgeben darf, egal, an wen und egal, ob persönlich oder am Telefon!

Mit ist bekannt, dass ich gegenüber meinem Arbeitgeber für den entstandenen Schaden hafte, wenn ich gegen diese Anweisungen verstoße und trotzdem Codes oder PIN-Nummern ohne vorherige Bezahlung herausgebe.

Die Mitarbeiterbelehrung zum e-loading-Betrug wurde mir am _____ persönlich ausgehändigt und erläutert.

X _____

gez. _____