

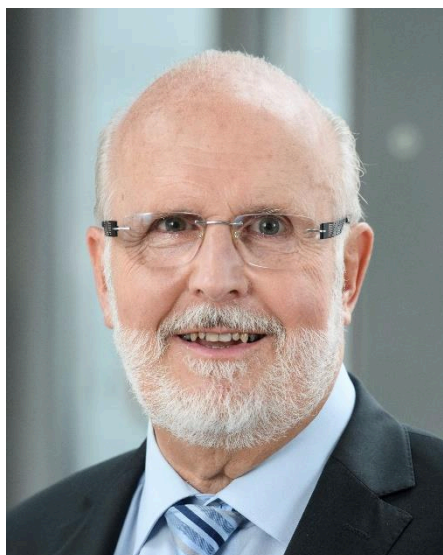
4/2024

Seniorenbrief

des VBE-Bundesverbandes

Sonderausgabe:

EC- und Kreditkartenbetrug



Liebe Kolleginnen und Kollegen,

in dieser Ausgabe widmen wir uns ausschließlich dem EC- und Kreditkartenbetrug. Sie erfahren Tipps zum sicheren Umgang mit Zahlungskarten, was Sie tun können beim Verlust der Karte und wie man eine entwendete Karte sperren kann.

Außerdem gibt es wieder einen heiteren Beitrag in Sütterlin-Schrift. Lassen Sie sich überraschen.

Ich wünsche Ihnen viel Spaß beim Lesen.

Ihr

Max Schindlbeck

VBE-Bundesseniorensprecher

EC- und Kreditkartenbetrug

EC- und Kreditkarten sind eine gängige Alternative zum Bargeld und besitzen als Zahlungsmittel eine recht hohe Akzeptanz - auch international. Diesen Umstand machen sich auch Kriminelle zu Nutze und entwickeln immer neue Vorgehensweisen, um an sensible Daten, wie PINs oder Kartenprüfnummern zu kommen. Skimming und Phishing zum Beispiel.

Auf den folgenden Seiten erfahren Sie mehr über den sicheren Umgang mit unbaren Zahlungsmitteln und Möglichkeiten, wie Sie sich vor EC- und Kreditkartenbetrug schützen. So besteht bei Diebstahl oder Verlust einer Debitkarte die Möglichkeit, über den zentralen Sperr-Notruf 116 116 oder durch die Polizei eine Debitkarte unverzüglich für weitere Zahlungen sperren zu lassen.

Vorsicht beim bargeldlosen Bezahlen

EC- und Kreditkarten spielen beim bargeldlosen Bezahlen in den verschiedensten Bereichen eine Rolle: Sie können als Alternative zum Bargeld bequem als Zahlungsmittel eingesetzt werden. Hinzu kommt die weltweite Akzeptanz von Kreditkarten im Handel, sowie die Möglichkeit, an über 1,7 Millionen Geldausgabeautomaten (ca. 60.000 in Deutschland) Bargeld mittels EC-Karte/Bankkarte bzw. Kreditkarte abzuheben.

Die starke Verbreitung und vor allem die hohe Akzeptanz des "Plastikgeldes" üben auf Straftäter eine unwiderstehliche Anziehung aus - der EC- und Kreditkartenbetrug floriert. Dabei wird es Kriminellen oft leicht gemacht: Daten wie die Kreditkartennummer, die Gültigkeitsdauer der Karte und die Unterschrift gibt ein Kreditkartennutzer überall dort preis, wo er per Karte zahlt. Alle Daten sind Bestandteil der Quittung. So kommen mit jeder Zahlung mehr und mehr Menschen in den Besitz höchst vertraulicher Informationen.

Des Weiteren entwickeln Täter neue Vorgehensweisen, um betrügerisch an Kartendaten und persönliche Geheimzahl zu gelangen - wie z.B. das so genannte Skimming.

Betrug mit Zahlungskarten

Beim Betrug mit Zahlungskarten (z.B. Girocard, früher auch als ec-Karte bezeichnet) mit PIN steigen die Zahlen 2022 mit 25.351 Fällen gegenüber 2021 mit 22.226 Fällen an. Betrugsfälle mit rechtswidrig erlangten Zahlungskarten ohne PIN stiegen erneut an, von 12.331 Fällen auf 17.457 Fälle (2020: 12.241

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

Fälle). Mehr Informationen zu den Fallzahlen finden Sie im Infotext zu Zahlungskartenbetrug.

Bezahlen mit Kreditkarten Internet

Bei dieser Bezahlmöglichkeit werden Waren oder Leistungen per Schreiben, Telefon, Fax bzw. hauptsächlich über das Internet bestellt. Die Bezahlung erfolgt unter Angabe der Kreditkartennummer und des Verfalldatums, gegebenenfalls zusätzlich mittels der dreistelligen Kartenprüfnummer (CVC/CVV; auf der Kartenrückseite).

Aktuell nutzen in Deutschland ca. 80 Prozent aller Personen ab 10 Jahren das Internet zu Hause, am Arbeitsplatz oder anderswo. Die starke Verbreitung des Internets machen sich auch Kriminelle zu Nutze, um an Daten von Zahlungskarten zu kommen: So geben unseriöse Händler beim Einsatz von Kreditkarten(-daten) im Internet nach Abschluss des Geschäfts die Kartendaten weiter oder nutzen sie illegal. Ebenso können Dritte bei einer unverschlüsselten Internetverbindung Kartendaten von Privatpersonen oder Firmen abgreifen.

Auch durch gefälschte Internetmails oder mittels Viren und Schadprogrammen (Trojaner) versuchen Betrüger, an Zahlungskartendaten, Passwörter oder persönliche Daten zu gelangen (Phishing).

Worauf Sie beim Onlineshopping achten sollten, haben wir in unseren Tipps für einen sicheren Online-Kauf zusammengefasst.

Tipps zum sicheren Umgang mit Zahlungskarten

Umgang mit der PIN

- Die **PIN darf nie an Dritte** weitergegeben werden, nicht einmal Geldinstitute oder Kreditkartenunternehmen kennen die PIN; weder Amtspersonen (z.B. Polizeibeamte) noch Mitarbeiter von Geldinstituten werden deshalb legal nach der PIN fragen.
- Lernen Sie am besten Ihre **PIN auswendig** und **vernichten Sie den PIN-Brief**.
- **Auf keinen Fall sollte die PIN irgendwo notiert** werden - schon gar nicht auf der Zahlungskarte! Auch nicht im Adressbuch getarnt als Telefonnummer o.ä.
- Achten Sie bei der **Eingabe der PIN** am Geldausgabeautomaten oder im Handel am Kassensystem darauf, dass **niemand den Vorgang beobachten kann**; bitten Sie aufdringliche Personen oder angebliche Helfer höflich aber bestimmt, auf Distanz zu bleiben.

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

- **Verdecken Sie die PIN-Eingabe**, indem Sie die Hand oder Geldbörse als Sichtschutz dicht über die Tastatur halten. Dies erschwert ein Ausspähen erheblich.
- Geben Sie die **PIN niemals an Türöffnern**, auch nicht bei Banken, ein. Verständigen Sie in solchen Fällen sofort die Polizei.
- Befolgen Sie **keine Hinweiszettel, die zur mehrmaligen Eingabe der PIN** auffordern.
- Geben Sie **beim Bezahlen nicht die PIN bekannt** und achten Sie auf die Rückgabe der eigenen Zahlungskarte.

Allgemeine Empfehlungen

- Lassen Sie **Zahlungskarten niemals in Büro-/Arbeitsräumen, Schwimmbädern, Krankenhäusern, Hotelzimmern, Kraftfahrzeugen etc. liegen** - weder offen noch versteckt; auch nicht für nur kurze Zeit.
- Behandeln Sie EC- und Kreditkarten vielmehr sorgfältig wie Bargeld und tragen Sie sie in verschlossenen Innentaschen der Kleidung verteilt dicht am Körper.
- Überzeugen Sie sich regelmäßig, ob Sie Ihre Karte(n) noch besitzen.
- Beobachten Sie bereits vor dem Geldabheben am Automaten Ihr Umfeld genau. **Achten Sie auf die äußere Beschaffenheit des Geldautomaten**, melden Sie auffällige Veränderungen am Geldautomaten sofort der Polizei. Begeben Sie sich niemals gedankenlos zum Geldabheben an den Automaten.
- Beachten Sie alle **Auflagen, die Ihr Geld- oder Kreditinstitut vertraglich mit Ihnen vereinbart** hat. Lesen Sie auch das Kleingedruckte im Vertrag – vor allem die Abschnitte über die Haftung; sie legen fest, welche Sorgfaltspflichten Sie im Umgang mit Ihrer Zahlungskarte zu erfüllen haben.

- Bewahren Sie **Kreditkarten-/Bankkartenbelege sorgfältig auf und kontrollieren Sie Ihren Kontoauszug zeitnah**. Vernichten Sie verschriebene Belege, unter Umständen auch das Durchschreibepapier.
- Behalten Sie Ihre Karte stets im Auge.

Zahlungskarten im Internet

- Bei Internet-Transaktionen ist generell die Internet-Sicherheit zu beachten, d.h. verwenden Sie immer ein aktuelles Virenschutzprogramm und eine aktuelle Firewall, überprüfen Sie Browsereinstellungen,

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

insbesondere hinsichtlich aktiver Inhalte. Öffnen Sie **keine E-Mails von unbekanntem** Absendern. Führen Sie die Transaktion möglichst am eigenen Rechner aus. Mehr Infos unter Sicherheitskompass.

- Geben Sie Ihre Kreditkartennummer nur über Verbindungen weiter, die eine **Verschlüsselung zwischen Ihrem Rechner und dem Empfänger** gewährleisten (z.B. SSL-Standard).
- Zudem kann zusätzlich die Angabe der Kartenprüfnummer (bei VISA heißt sie CVV2= Card Verification Value 2, bei Mastercard CVC2=Card Verification Code 2) gefordert werden, die auf der Kreditkarte selbst aufgedruckt ist, aber nicht im Magnetstreifen gespeichert ist.
- **Allgemein gilt: Versichern Sie sich, mit wem Sie es zu tun haben.** Drucken Sie die Allgemeinen Geschäftsbedingungen und das Impressum (Adressenangabe, Telefonnummer) aus. Überprüfen Sie anhand der Angaben die Existenz des Internet-Unternehmens. Drucken Sie den kompletten Geschäftsvorgang aus. Beachten Sie bei Internet-Händlern mit Sitz im Ausland, insbesondere in Nicht-EU-Staaten, dass unser Rechtssystem möglicherweise keinen Zugriff hat. Wählen Sie ggf. andere Zahlungsmöglichkeiten aus (per Nachnahme, per Lastschrift, per Überweisung).

Weitere nützliche Informationen finden Sie im Faltblatt "Vorsicht Karten-Tricks" oder auf den Seiten von www.kartensicherheit.de. So kann man dort unter anderem einen so genannten SOS-Infopass herunterladen.

Die Karte ist weg - was tun?

Den weit verbreiteten Einsatz des „Plastikgeldes“ machen sich viele Täter zu eigen. Lassen Sie Ihre Karte bei Verlust deshalb sofort für den weiteren Gebrauch sperren, auch wenn diese aus nicht nachvollziehbaren Gründen vom Geldautomaten einbehalten wird.

Bei Verdacht auf eine Straftat sollte ebenfalls sofort Anzeige bei der Polizei erstattet werden.

KUNO - Debit-Karten für Lastschriftverfahren sperren

Mehr Sicherheit im unbaren Zahlungsverkehr wird durch ein computergestütztes System der Polizei gegen den Missbrauch von gestohlenen ec-Karten erreicht.

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

KUNO (Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen) ist ein freiwilliges System der Polizeibehörden und der Wirtschaft. Ziel ist, Betrugsfälle im kartengestützten Zahlungsverkehr zu reduzieren.

Nach dem Verlust Ihrer Debitkarte (z.B. girocard, früher auch als ec-Karte bezeichnet) sollten Sie diese nicht nur bei Ihrer Bank sperren lassen, sondern auch bei der Polizei als gestohlen melden! Die Polizei meldet dann die Daten Ihrer abhanden gekommenen Debitkarte (Bankleitzahl, Kontonummer und Kartenfolgenummer) dem Kooperationspartner des Einzelhandels. Von dort werden diese Daten an die dem KUNO-Sperrsystem angeschlossenen Einzelhandelsgeschäfte weitergeleitet. Nur so ist Ihre Karte auch für das Lastschriftverfahren (Bezahlen mittels Karte plus Unterschrift) gesperrt!

Sperr-Notruf 116 116

Aufgrund der steigenden Zahl von kartenbasierten Zahlungen und der daraus resultierenden Unübersichtlichkeit von Sperr-Hotlines wurde auf Empfehlung des Bundesministeriums des Innern und als Projekt der Initiative D21 am 01. Juli 2005 der Sperr-Notruf 116 116 eingeführt.

Unterstützt wird die Kampagne vom Handelsverband Deutschland - Der Einzelhandel (HDE). Mit der Kampagne informieren die Aktionspartner den Verbraucher durch verstärkte Präventionsmaßnahmen und gezielte Tipps über das richtige Verhalten bei Kartenverlust, um so finanzielle Schäden zu verhindern.

Um den Missbrauch Ihrer Karten wirksam zu verhindern, sollten Sie Ihre gestohlenen oder verlorenen Karten sofort sperren lassen.

Debitkarten (z.B. girocard, früher auch als ec-Karte bezeichnet) können bundesweit über die einheitliche zentrale Telefonnummer 116 116 * (Sperr-Notruf) oder die 01805-021021 ** gesperrt werden.

Die Notrufnummer ist die weltweit erste zentrale und einheitliche Rufnummer, um Karten und elektronische Berechtigungen sperren zu lassen. Dem Bürger wird im Fall eines Kartenverlustes sicher, schnell und unkompliziert geholfen und darüber hinaus ist der Sperr-Notruf auch für sprach- und hörgeschädigte Menschen unter der Nummer 116 116 per Telefax erreichbar.

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

Seit dem 1. November 2010 besteht für Inhaber eines neuen Personalausweises oder elektronischen Aufenthaltstitels die Möglichkeit, die Sperrung der Online-Ausweisfunktion telefonisch zu veranlassen

Aus dem Ausland erreichen Sie den Sperr-Notruf mit der jeweiligen Landesvorwahl für Deutschland, in der Regel unter +49 116 116. Zur zusätzlichen Sicherheit, insbesondere für die Erreichbarkeit aus dem Ausland, ist der Sperr-Notruf auch unter der Rufnummer +49 (0)30 40 50 40 50 zu erreichen.

Sperrnummern für Kreditkarten:

- MasterCard nur Deutschland: 0800 071 3542 *
- aus anderen Ländern (R-Gespräch): +1 636 7227 111
- Visa: 0800 811 8440 *
- aus anderen Ländern (R-Gespräch): +1 303 9671 096
- American Express: +49 69 97 97 1000 **
- Diners Club: +49 69 900 150 135 oder 136 **

* Kostenlos aus dem deutschen Festnetz und aus dem Mobilfunknetz innerhalb Deutschlands, abweichende Gebühren aus dem Ausland

** 14 Ct./Min. aus dem dt. Festnetz, 42 Ct./Min. Mobilfunkhöchstpreis, abweichende Gebühren aus dem Ausland

Bei einem Verlust empfehlen wir zudem, unverzüglich das kontoführende Institut zu benachrichtigen. Manche Institute bieten hierzu einen eigenen Notruf-Service an.

Was wird zur Sperrung benötigt?

Der Karteninhaber muss sich nicht für eine Nutzung des Sperr-Notrufs registrieren. Zur Sperrung der verlorenen Karten sollten dennoch folgende Daten bereit gehalten werden:

- EC- und Bankkarten: die Kontonummer wird unbedingt benötigt; die Bankleitzahl ist für die schnellere Abwicklung hilfreich
- Kreditkarten: der Name der Bank oder alternativ die Bankleitzahl

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

Welche Karten können gesperrt werden?

Der Sperr-Notruf 116 116 gilt für Kunden mit Karten oder Medien, deren Herausgeber sich dem Sperr-Notruf angeschlossen haben. Mittlerweile können über 116 116 mehr als 90 Prozent aller Bank- und Zahlungskarten, diverse Mitarbeiterausweise von Firmen und sogar Handy-Karten gesperrt werden. Die Konzeption des Sperr-Notruf sieht vor, Teilnehmer aus anderen Branchen und mit anderen Medien, z.B. aus dem Gesundheitswesen, sowie Unternehmen mit Mitarbeiterausweisen oder Zugangsberechtigungen einzubinden. Der diskriminierungsfreie Zugang ermöglicht es, dass sich alle Herausgeber von Karten und elektronischen Berechtigungen dem Sperr-Notruf anschließen können - unabhängig von der Anzahl der im Umlauf befindlichen Karten.

Aus der Homepage der
Polizeilichen Kriminalprävention
der Länder und des Bundes
www.polizei-beratung.de

Heitere und nachdenkliche Lehrer geschichten aus früheren Zeiten, geschrieben in altdeutscher Schrift:

General Müller

Als nach dem 2. Weltkrieg die Lehrerstellen in Bayern wieder besetzt wurden, erhielt ein ehemaliger General mit Namen Müller die Hauptlehrerstelle an einer schwäbischen Dorfschule. Von seinen Schülern und den Eltern wurde er stets ehrfurchtsvoll als „Herr General“ angesprochen. Dienstvorgesetzter war ein gewisser Schulrat Berkel, ehemals Oberst a.D. Deshalb kommentierte Müller alle Weisungen aus dem Schulamt mit dem Satz: „Was will der geschissene Oberst schon wieder?“

Eines Tages nun bekam Hauptlehrer Müller Besuch von Berkel in Begleitung eines Amtrates von der Regierung von Schwaben. Anlass war eine geplante Schulhauserweiterung. Man traf General Müller Pfeife rauchend in seinem Klassenzimmer an. Zunächst unterhielt man sich über die geplante Baumaßnahme.

Am Ende des Gesprächs bat der zuständige Schulrat „Oberst“ Berkel den General a.D., darüber nachzudenken, ob der Tabakrauch für die Schüler nicht gesundheitsgefährdend sei. Die Antwort des Angesprochenen kam in militärischem Ton: „Meine Herr, was ist pädagogisch besser? Wenn mich so ein halbstarker Kerl in dieser Klasse bis aufs Blut ärgert, soll ich ihn dann grün und blau schlagen? Oder ist es nicht sinnvoller, in meine Pfeife zu beißen und im Unterricht fortzufahren?“ Mit dieser Äußerung beendete Müller das Gespräch und ging rauchend wieder in sein Klassenzimmer zurück.

Max Schindlbeck

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

General Müller

Als noch im 2. Weltkrieg in Lagerhallen in
Lagern wieder besetzt wurden, wird ein sta-
maliger General mit Namen Müller in Höngg-
Lagerhalle an einer physikalischen Vorlesung.
Von seinen Schülern und dem Lehrer werden er
1946 als "Herr General" angespro-
chen. Dienstverpflichteter war ein gewisser Schül-
ter Lutzel, damals Oberst u. d. Inhab der Pommern-
straße Müller alle Maßnahmen und dem Schüleramt
mit dem Satz: „Was will der gewöhnliche Oberst
von mir?“

Einmal fand man beim Höngg-Lager Müller
Lutzel von Lutzel in Begleitung eines Amte-
rates von der Regierung von Schwaben. Anlaß
war eine geplante Schülerüberweisung.
Man traf General Müller heute während in
seinem Klassenzimmer an. Zunächst unter-
sucht man sich über die geplante Überweisung
nach.

Am Ende des Gesprächs hat der zuständige Schül-
ter „Oberst“ Lutzel dem General u. d. Vorüber
nachzufragen, ob der Überweisung für die
Schüler nicht gesundheitlich gefährlich sei. In
Antwort des Angewandten Pans in militä-
rischem Ton: „Mein Herr, was ist gesundheitlich
besser? Wenn mich so ein halber Oberst Lutzel
in dieser Klasse bis zum Ende bringt, soll ich

Bundesseniorenvertretung

im Verband Bildung und Erziehung

Bundessprecher: Max Schindlbeck, Mozartstr.9, 86470 Thannhausen

ist dem grün und blau pflügen? Oder ist es
 nicht sinnvoller, in meine Hände zu greifen und
 im Unterricht fortzuführen? Mit dieser Über-
 rüfung bewies Müller das Gegenteil und ging
 konsequent wieder in sein Klassenzimmer zurück.

Max Schindlbeck

Vielleicht hatten Sie während Ihrer Schulzeit auch ein nettes Erlebnis, das Sie aufschreiben und uns schicken könnten. Ich würde mich sehr über Ihre Lehrer Geschichte freuen. Bitte schicken Sie Ihren Beitrag in normaler Druckschrift (am besten als Word-Datei) an:

Max Schindlbeck, Mozartstraße 9, 86470 Thannhausen,

Tel: 08281 5655, Fax: 08281 5676, E-Mail: m.schindlbeck@vbe.de

Alle Beiträge wurden nach bestem Wissen und Gewissen erstellt. Dennoch kann eine juristische Gewähr für die Richtigkeit dieser Angaben nicht übernommen werden. Eine Haftung in diesem Zusammenhang ist ausgeschlossen.