



[Erschreckende Symptome nach Drogenkonsum auf Ferieninseln >](#)
[< Unseriöse Schlüsseldienste](#)

Sicherheit bei Online-Bezahldiensten

Geschickte Betrüger, überrumpelte Opfer



Onlinebezahlsysteme können z.B. in Kiosken und Tankstellen gekauft werden

© paysafecard Deutschland GmbH

Prepaid-Online-Zahlungsmittel wie paysafecard oder Ukash werden als alternative Bezahlsysteme im **Internet** immer beliebter. Der Vorteil: Man kann auch kleine Beträge bei Online-Käufen bequem bezahlen, ohne dabei private Daten wie Name oder Kontoverbindung angeben zu müssen. Aber auch für Betrüger sind die digitalen Zahlungsmittel attraktiv: Kommen sie etwa in Besitz von PINs, die der Kunde für seine Käufe nutzt, können sie selbst damit im **Internet** auf Shoppingtour gehen. Häufig werden die PINs auch im großen Stil durch Betrügereien und Erpressungen erlangt und am Ende „ausgecasht“, also wieder in Bargeld umgewandelt.

Betrüger sind dreist und einfallsreich

Angriffsszenarien im Bereich Online-Bezahlsysteme gibt es viele. Ziel von Betrügern sind dabei einerseits die Ausgabestellen der PINs, also das Kassenspersonal in Supermärkten oder an Tankstellen, aber auch die Nutzer selbst. Ziel ist es dabei immer, an PINs zu kommen. „Die Betrüger gehen dabei sehr geschickt vor und versuchen entweder, Druck bei den Opfern aufzubauen oder sie mit finanziellen Vorteilen zu locken“, erklärt Bernd Fox aus dem Sachbereich „Organisierte Kriminalität“ der Polizeidirektion Osnabrück. Häufig seien zum Beispiel Gewinnversprechen, bei denen gezielt ältere Menschen angerufen und zu Geldzahlungen per Online-Bezahlsystem aufgefordert würden. Die Betrüger erklären den Opfern, dass sie

erst eine bestimmte Summe zahlen müssten, bevor ein Gewinn ausgeschüttet werden könne. Da das Geld aus dem Ausland komme und dort Steuern beglichen werden müssten, solle dazu das Online-Bezahlsystem genutzt werden. Die **Opfer** geben dann die geldwerten PINs an die Betrüger heraus. Aber auch bei so genannter „Ransomware“, also Software, die von Kriminellen eingesetzt wird, um Computernutzer zu erpressen, wird als Zahlungsmittel unter anderem paysafecard genutzt. Bei einem solchen Angriff erscheint auf dem Rechner zum Beispiel die Meldung, dass man illegale Musikdownloads oder kinderpornografisches Material auf dem Rechner hätte und deshalb **Strafe** zahlen müsse. Oder die Festplatte wird verschlüsselt und die Angreifer drohen damit, die Daten zu löschen, falls man nicht die geforderte Summe zahlt. „Voraussetzung für solch einen Angriff ist die vorherige Infektion des Rechners mit Schadsoftware – etwa über manipulierte Webseiten oder infizierte E-Mail-Anhänge“, erklärt Bernd Fox. „Die **Opfer** eines solchen Erpressungsversuchs sind meist völlig überrumpelt und zahlen die geforderte Summe, weil sie Angst um ihre Daten haben. Es gibt Fälle, bei denen **Opfer** 3.000 Euro in Form von PINs gezahlt haben“, so der Experte. Bei weiteren Betrugsvarianten geht es beispielsweise um den Erlass von Schulden oder aber darum, das Guthaben einer paysafecard vermeintlich zu verdoppeln. „Der Kreativität der Betrüger sind dabei keine Grenzen gesetzt“, so Fox. Eine beliebte Masche beim **Betrug** an den Verkaufsstellen: Ein Anrufer täuscht vor, Angestellter des paysafecard-Technikservices zu sein. Er gibt zum Beispiel vor, dass es beim Generieren der PINs ein Problem gibt und fordert den Kassierer auf, testweise Codes zu generieren und diese telefonisch durchzugeben. „Obwohl unsere Distributoren und das Kassenpersonal ausführlich und intensiv geschult werden sowie ausführliche Informationsmaterialien erhalten, kommt es immer wieder dazu, dass PINs am Telefon herausgegeben werden. Die Betrüger haben sich auf diese Anrufe gut vorbereitet und verfügen zum Teil über gut recherchierte Informationen – wie etwa Namen von Vorgesetzten oder interne Abläufe“, weiß Maximilian von Both.

Vorgehen im Betrugsfall

Wurde eine **PIN** an Betrüger herausgegeben, kommt es vor allem auf eines an: Schnelligkeit. Denn es besteht die Möglichkeit, den Code beim Anbieter sperren zu lassen, noch bevor die Betrüger ihn einlösen können. „Wenn die betroffene Person selbst noch keinen Kontakt zum Anbieter des Bezahlendienstes aufgenommen hat, sollte dies spätestens der Beamte tun, der die Anzeige aufnimmt“, betont Bernd Fox. „Der erste Ansatz muss sein, den Schaden so gering wie möglich zu halten und zu versuchen, ob noch etwas zu retten ist. Kennt man sich mit der Bearbeitung solcher Fälle nicht gut aus, sollte man unbedingt einen erfahrenen Kollegen hinzuziehen“, so der Experte. Im Weiteren muss geklärt werden, wie der **Betrug** vonstatten ging. Handelt es sich um einen Erpressungsversuch, bei dem der Rechner infiziert wurde? Oder wurde man per Post mit einem Gewinnversprechen angeschrieben? „Für Erpressungsopfer haben wir ein Merkblatt vorbereitet, das wir den Betroffenen schicken können. Darin werden wichtige Angaben zur Straftat erläutert und aufgezeigt, was der Betroffene jetzt tun sollte, etwa, wie der „gesperrte“ PC ggf. wieder lauffähig gemacht werden kann. Der Betroffene sollte vor der Rücksprache mit der **Polizei** keine Veränderungen am PC vornehmen und der **Polizei** mitteilen, womit die Täter drohen, welches Bezahlssystem genutzt werden soll und ob zusätzlich eine alternative E-Mail-Adresse als Kontakt angegeben ist. Es ist außerdem hilfreich, wenn der Betroffene den Bildschirm mit der konkreten Forderung fotografiert und uns das Foto für weitere Ermittlungen zur Verfügung stellt“, so Fox. Wichtig dabei: Die Beamten sollten immer darauf hinweisen, dass kinderpornografisches Material, das bei solchen Erpressungsversuchen gelegentlich mit abgebildet wird, beim Fotografieren abgedeckt werden muss, da man

ZUM SICHEREN UMGANG MIT ONLINE-BEZAHLDIENSTEN:

Um diese Dienste sicher nutzen zu können, ist es dringend notwendig, sich an die Sicherheitsanforderungen und -anweisungen des jeweiligen Anbieters zu halten, z.B.: Die **PIN** nur bei offiziellen Verkaufsshops einkaufen; niemals die **PIN** per Mail oder am Telefon herausgeben; bei Internetkäufen die **PIN** nur in autorisierten Online-Shops einsetzen; im Betrugsfall schnell den Anbieter kontaktieren. Mehr Infos zur Sicherheit bei der Nutzung von Online-Bezahlssystemen gibt es in der Regel beim jeweiligen Anbieter.

sich sonst aufgrund des Abspeicherns oder Ausdrucken von **Kinderpornografie** strafbar machen kann

Interessant ist auch die Frage, wie der Virus auf den Rechner gekommen ist: Wurde eine bestimmte Webseite besucht? Oder hat man einen infizierten E-Mail-Anhang geöffnet? „Je mehr Informationen man über den Hergang sammelt, desto besser. Das ist sehr hilfreich für die Fragestellung, ob es sich um einen bekannten oder einen neuen Trojaner handelt. Nicht zuletzt sollten die Kollegen die Betroffenen aber auch noch einmal über grundlegende IT-Sicherheit aufklären bzw. Hinweise zur sicheren Nutzung von Online-Bezahlungssystemen geben“, betont Bernd Fox.



[Alle Artikel dieser Kategorie](#)

© Verlag Deutsche Polizeiliteratur

Cookie Einstellungen

- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer [Datenschutzerklärung](#) beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

Nur essentielle Cookies akzeptieren Alle akzeptieren