Fürstlich Castell'sche Bank

Sicherheit im Online-Banking.

FÜRSTLICH CASTELL'SCHE
BANK

Fürstlich Castell'sche Bank
Sicherheit im Online-Banking.

Inhalt

Sicherheitstipps
Bitte unbedingt beachten:

PIN und TAN sind wie Bargeld zu behandeln. Sie sollten deshalb unbedingt getrennt voneinander und unter Verschluss aufbewahrt werden.

Achten Sie darauf, dass während des gesamten Online-Banking-Dialogs des Sicherheitssymbol Ihres Browsers auf aktiv steht. (Nur gültig für Online-Banking (HBCI mit PIN und TAN)).

Die PIN ist für Sie der elektronische Ausweis, um sich zu legitimieren. Nachdem Sie uns den Empfang bestätigt haben, müssen Sie die PIN beim Erstzugang zu Ihrem Konto ändern. Sie sollten keine leicht zu ermittelnde PIN verwenden (z.B. nicht Ihr Geburtsdatum).

Jede TAN kann nur einmal verwendet werden.

Sicherheitstipps

Vorsicht vor Angriffen auf PIN und TAN

Vorsicht vor Betrügern und Trojaner-Angriffen auf PIN und TAN.Trojaner versuchen unbemerkt von Ihnen, die Sicherungsmittel zum Online-Banking (PIN und TAN) auszuspähen. Weiterhin könnten Kunden der Fürstlich Castell'schen Bank E-Mails erhalten, in denen sie dazu angeregt werden, ihre Zugangsdaten in manipulierten Formularen einzugeben und zu versenden. Bitte beachten Sie, dass die Fürstlich Castell'sche Bank Sie niemals per E-Mail auffordern wird, sensible Kundendaten zur Überprüfung im Internet einzugeben.

Was sind Trojaner?
Wie greifen Trojaner das Online-Banking an?
Wie schützen Sie sich vor Trojanern?
Was ist Phishing?
Wie erkennen Sie Phishing?
Wie schützen Sie sich vor Phishing?
Sie benötigen weitere Informationen?

Was sind Trojaner?
Betrüger versuchen nun neben Phishing-Attacken mit Trojanern an Ihre Online-Banking-Sicherungsmittel PIN und TAN zu gelangen. Dazu werden auf Ihrem PC Programme unbemerkt eingeschleust (Trojaner), die Schwachstellen in Browsern ausnutzen, Ihre PIN und TAN bei der Eingabe im Online-Banking ausspähen und anschließend an kriminelle Betrüger weiterleiten.

Wie greifen Trojaner das Online-Banking an?
Nach den uns vorliegenden Informationen verhält sich der infizierte pc dabei bis zur Eingabe der tan unauffällig. Erst nach Eingabe der Transaktionsnummer wird die Verbindung zum Online-Banking-Server abgebrochen. Ein erneuter Verbindungsaufbau zur Online-Banking-Seite über diesen Browser scheitert. Währenddessen übermittelt der installierte Trojaner die Benutzerdaten an den Angreifer.

Wie schützen Sie sich vor Trojanern?
Installieren Sie konsequent die für Windows verfügbaren Sicherheits-Updates. Setzen Sie Virenscanner und ergänzend Firewalls ein. Aktualisieren Sie regelmäßig Ihren Virenscanner und Ihre Firewalls. Sollte Ihre Session während des Online-Bankings nach Eingabe von PIN und TAN unterbrochen werden, sollten Sie grundsätzlich misstrauisch werden. Im Zweifelsfall sollten Sie sich umgehend mit Ihrem Berater der Fürstlich Castell'schen Bank in Verbindung setzen und in jedem Fall Ihre Kontoumsätze prüfen.

Was ist Phishing?
Phishing ist ein Kunstwort aus »Password« und »fishing« und steht für das Fischen von Passwörtern. Dabei versuchen Betrüger, z.B. an Ihre Zugangsdaten zum Online-Banking zu gelangen. In einer gefälschten Mail, die den Anschein einer E-Mail der Fürstlich Castell'schen Bank erweckt, wird versucht, Sie per Link auf eine manipulierte Webseite zu leiten. Auf dieser gefälschten Webseite erfolgt dann die Aufforderung, persönliche Kundendaten, wie z.B. Ihre Online-Kennung, PIN (Persönliche Identifikationsnummer) und eine gültige TAN (Transaktionsnummer) einzugeben. Bis heute ist uns keine Phishing-Aktion zu Lasten der Fürstlich Castell'schen Bank bzw. der Kunden der Fürstlich Castell'schen Bank bekannt geworden.

Wie erkennen Sie Phishing?
Die Fürstlich Castell'sche Bank wird Sie niemals per E-Mail auffordern, sensible Kundendaten zur Überprüfung im Internet einzugeben. Sie werden ebenso niemals E-Mails erhalten, die Sie veranlassen Webseiten zu öffnen und dort Kundendaten einzugeben, die nicht zweifelsfrei der Fürstlich Castell'schen Bank zuzuordnen sind. Auch per Telefon werden wir Sie nie nach sensiblen Daten wie Ihre PIN oder TAN fragen.

Wie schützen Sie sich vor Phishing?
Um sich vor Phishing zu schützen, ist vor allem Ihre Aufmerksamkeit gefragt. Geben Sie auf keinen Fall Ihre persönlichen Daten wie z.B. Kreditkartennummer, Geheimnummer zu Ihrer Maestro-Bankkarte oder Ihre Zugangsdaten zum Online-Banking auf Webseiten ein, wenn Sie per E-Mail dazu aufgefordert werden. Verlassen Sie sich nicht auf das Aussehen der Seite, sondern prüfen Sie dazu auch deren Echtheit. Sollten Sie bereits auf eine solche E-Mail geantwortet oder nach Anklicken eines solchen Links vertrauliche Daten eingegeben haben, empfehlen wir Ihnen umgehend Ihre PIN im Online-Banking zu ändern. Im Zweifelsfall sollten Sie sich umgehend mit Ihrem Berater der Fürstlich Castell'schen Bank in Verbindung setzen und in jedem Fall Ihre Kontoumsätze prüfen.

Sicherheitstipps

So könnte ein betrügerischer E-Mail Text aussehen:

Sehr geehrter <Kunde>,

die Fürstlich Castell'sche Bank ist stets bemüht, ihr Online-Banking so attraktiv wie möglich zu gestalten. Aus diesem Grund haben wir unsere Online-Banking Systeme weiterentwickelt.

Nun ist es erforderlich, die einwandfreie Funktion unserer neuen Systeme zu überprüfen.

Um sicherzustellen, dass Sie auch in Zukunft einen fehlerfreien Zugriff auf ihr Konto haben, bitten wir Sie daher, Ihre Zugangsdaten zu prüfen. Geben Sie dazu einfach Ihre Online-Kennung, Ihre PIN *und eine gültige* TAN *in unser Prüfsystem ein. Folgen Sie dazu diesem Link. Sie erhalten sofort eine Bestätigung, ob Ihre Daten weiter Gültigkeit besitzen.*

Mit freundlichen Grüßen

Fürstlich Castell'sche Bank
Kundenservice.

Sollten Sie bereits auf eine solche E-Mail geantwortet oder nach Anklicken eines solchen Links vertrauliche Daten eingegeben haben, empfehlen wir Ihnen dringend, umgehend Ihre PIN für das Online-Banking zu ändern. Bitte wenden Sie sich im Zweifelsfall schnellstmöglich an Ihren Berater der Fürstlich Castell'schen Bank.

Sicherheitstipps

Tipps zur Sicherheit gegen Phishing-Attacken

1. **Sichere Startposition**
Starten Sie Ihr Online-Banking ausschließlich durch die Eingabe der URL der Fürstlich Castell'schen Bank (http://www.castell-bank.de) oder durch den Aufruf über Ihre Favoritenliste.

2. **Verschlüsselung**
Die aufgerufenen Banking-Seiten sind immer SSL-verschlüsselt. Das angewandte Verschlüsselungs-Konzept stellt sicher, dass die Daten während der Übertragung nicht mitgelesen oder verändert werden können. Sie erkennen dies an dem Schloss-Symbol in der Statusleiste. Die Verschlüsselung erkennen Sie auch an der Bezeichnung https:// am Beginn der aufgerufenen Adresse. Das »s« in der Erweiterung des »http« weist darauf hin, dass eine gesicherte Daten-Übertragung stattfindet.

3. **Überprüfen Sie das Zertifikat zur Verschlüsselung**
Bei jedem Aufruf des Onlineg-Bankings ist das Zertifikat zu überprüfen. Damit wird gewährleistet, dass Sie auch tatsächlich mit der Fürstlich Castell'schen Bank kommunizieren. Durch einen Doppelklick auf das Schloss-Symbol finden Sie unter »Details« Angaben zur Gültigkeit, zur Zertifizierungsstelle, zum Fingerabdruck und zum Zertifizierungspfad.

4. **Ihre** PIN
Wählen Sie keine »Allerwelts-PIN«, sondern verwenden Sie möglichst eine schwer zu erratende Buchstaben/Zahlen-Kombination. Zahlenfolgen, der Vorname des Partners oder Geburtsdaten sind dabei wenig geeignet. Wechseln Sie Ihre PIN regelmäßig.

5. **Geheimhaltung**
Schützen Sie Ihre Kennwörter und Zugangsdaten. Speichern Sie diese auf keinen Fall auf Ihrem Rechner und verwahren Sie diese so, dass niemand darauf zugreifen kann.

6. **Aktualität**
Halten Sie das Windows-Betriebssystem aktuell. Führen Sie regelmäßig Updates durch. Ein aktuelles Programm bietet besseren Schutz.

7. **Sicherheitseinstellung und Virenscanner**
Aktivieren Sie die Sicherheitseinstellungen Ihres Browsers und achten Sie darauf, dass er die aktuellen Sicherheitsfunktionen beinhaltet. Verwenden Sie Sicherheitssoftware, zum Beispiel einen Virenscanner und eine Firewall.

8. **Nach dem Banking abmelden**
Nutzen Sie zu Ihrer eigenen Sicherheit immer die Funktion »Abmelden«, um Ihre Verbindung zum Online-Banking zu beenden. Erst mit dem Aufruf dieser Funktion wird Ihre Verbindung ordnungsgemäß getrennt.

9. **Überprüfen Sie regelmäßig Kontobewegungen**
Bei unklaren Buchungen oder einem Missbrauchsverdacht sperren Sie umgehend Ihren Online-Banking-Zugang (Telefonisch oder auch durch dreimalige Falscheingabe einer PIN) und setzen Sie sich so schnell wie möglich mit Ihrem Berater der Fürstlich Castell'schen Bank in Verbindung.

10. **Sicher ist sicher**
Beachten Sie regelmäßig die aktuellen Sicherheitshinweise vor Ihrer Anmeldung zum Online-Banking.

Auf unterschiedlichen Wegen an das gleiche Ziel

Wie sicher ist Online-Banking?

Diese Frage stellt sich den Bankkunden angesichts von fortschreitenden Phishing-Attacken immer häufiger. Dabei bietet Ihnen Online-Banking zahlreiche Vorteile – von reduzierten Kosten bis hin zu mehr Flexibilität.

Verfahren mit dem Plus an Sicherheit

Im Zuge der permanenten Optimierung entstand bis heute ein Angebot an Lösungen rund um die Abwicklung des Online-Bankings und die Generierung von TANs und Signaturen, die unterschiedlichste Anforderungen berücksichtigen.

Da sich die Angriffsszenarien ändern, müssen die Sicherheitsverfahren entsprechend angepasst werden. Das ist auch der Grund dafür, dass in regelmäßigen Abständen neue Verfahren auf den Markt kommen. Nur so kann die Sicherheit gewährleistet und Ihr Vertrauen in das Online-Banking gefestigt werden.

Gefahren kennen
Ängste bannen

Immer wieder sind in den Medien die vielfältigen Risiken für Online-Banking und Online-Geschäfte ein Thema. Je besser Sie diese möglichen Gefahren kennen, desto leichter fällt es Ihnen diese einzuschätzen. Hier eine Übersicht über einige unerwünschte Vorgehensweisen und Versuche, unberechtigt an Daten zu gelangen.

Backdoors Im übertragenen Sinn durch die Hintertür kommen die »Backdoors« genannten Teile von Programmen. Mit ihrer Hilfe versuchen Hacker, unberechtigt Zugang zu PC's zu erhalten.

Computerviren Weitgehend bekannt sind »Computerviren«; diese verbreiten sich selbst, schleusen sich in andere Programme ein und vervielfachen sich auf diese Weise.

Computerwürmer »Computerwürmer« verbreiten sich über ganze Netzwerke, z. B. per elektronischer Post, also E-Mails.

Flooding »Flooding« nennt sich das übermäßige automatisierte Versenden von Nachrichten, das Rechner komplett lahmlegen kann.

Keylogger Eine Software, die eingegebene Nutzerdaten wie etwa PINs oder Kennwörter protokolliert und weitersendet, heißt »Keylogger«.

Pharming Wird man im Internet auf eine gefälschte Website umgeleitet, wird dies »Pharming« genannt.

Phishing »Phishing« ist nach einigen spektakulären Missbrauchsversuchen in aller Munde. Es beschreibt den Versuch, über gefälschte Internet-Adressen an Daten eines Users zu gelangen.

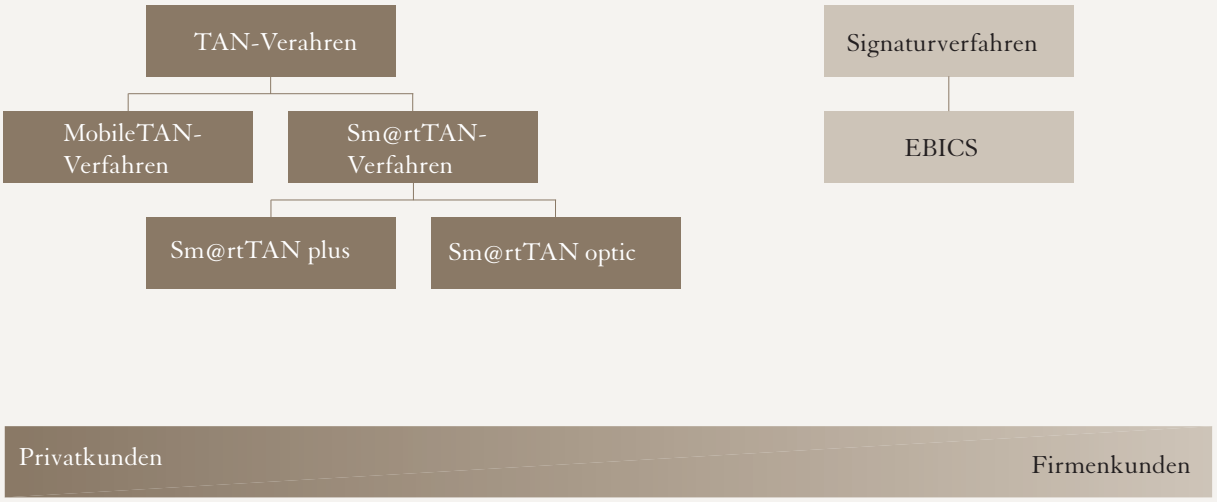
Ransomware Hin und wieder wurden auch schon Computer von außen verschlüsselt - per »Ransomware«. Im Anschluss gab es dann eine Art Lösegeldforderung mit dem Versprechen auf Entschlüsselung.

Rootkits Vorsicht vor »Rootkits«: Diese Programem ermöglichen Einbrechern in Computersysteme, weitere Einbrüche ins System zu verschleiern.

Spoofing Wer fälscherlicherweise Vertrauenswürdigkeit vorgibt, um Betrug im Netz vorzubereiten, nutzt das so genannte »Spoofing« - bspw. durch durch Manipulation seiner vorgeblichen Adresse.

Unterschiedlich - und doch in einem gleich *Im Anspruch auf Sicherheit*

Grundsätzlich haben Sm@rtTAN und mobileTAN in der Online-Filiale gemeinsam, dass Ihnen in einer sicheren Umgebung ihre Transaktionen zur Kontrolle angezeigt werden und die Auftragsdaten an die TAN gebunden sind. Der Unterschied liegt zum einen in der Handhabung (manuelle oder optische Eingabe) und in der Genauigkeit der angezeigten Geschäftsvorfallsdaten.



TAN-Generierung mit Hilfe eines Handys/Smartphones

mobileTAN

Handy/Smartphone-Besitzer haben die Möglichkeit, ihre TAN auf ihr Telefon senden zu lassen. Zunächst werden Sie in der Bank für das Verfahren freigeschaltet. Hierzu geben Sie für die spätere Zusendung der TAN auf Ihr Handy eine entsprechende Handynummer an. Die Anmeldung im Online-Banking läuft wie gewohnt. Erst kurz vor der Ausführung der Online-Transaktion erhalten Sie die mobileTAN per SMS auf das registrierte Handy/Smartphone geschickt. Nach Überprüfung der in der SMS enthaltenen Daten auf ihre Richtigkeit (bei einer Überweisung z. B. Betrag, Kontonummer, Zeit) geben Sie die mobileTAN in die Anwendung ein.

Viele gute Gründe für mobileTAN.

Die mobileTAN steigert die Sicherheit der Transaktion, indem zwei Kommunikationsmedien (Computer und Handy/Smartphone) eingesetzt werden. Die jeweilige TAN ist nur für die aktuelle Transaktion gültig und kann nicht für andere Transaktionen missbraucht werden. Die SMS-Daten, wie etwa die Kontonummer des Begünstigten und der Betrag, dienen der Kontrolle durch Sie. Wer sein Handy/Smartphone in der Regel bei sich trägt, verfügt mit mobileTAN über eine sehr flexible Lösung, die es ermöglicht, von jedem Computer mit Internet-Zugang die eigenen Bankgeschäfte abzuwickeln.

In zwei Schritten zur TAN
Sm@rtTAN plus - mit dem Mehr an Sicherheit

In zwei Schritten zur TAN und damit zum möglichst sicheren Online-Banking:

Dies funktioniert mit Sm@rtTAN plus. Für die Anwendung des Verfahrens benötigen Sie ein spezielles Lesegerät, das Sie von uns erhalten. Mit Hilfe dieses Geräts können Sie über die Tastatur des Lesers die erforderlichen Eingaben tätigen. Die Auftragseinreichung erfolgt getrennt von der TAN-Übermittlung. So sorgt diese Verfahrenstrennung für zusätzliche Sicherheit. Die notwendigen Daten werden per Hand über die Tastatur des Lesers eingegeben.

Der Ablauf aus Ihrer Sicht:

– Erfassung der Überweisungsdaten im Online-Banking
– Übertragung der Daten an das System
– Prüfen, ob die auf dem Monitor angezeigten Kontext-Daten korrekt sind
– Eingabe des Start-Codes und der Kontextdaten (z. B. Kontonummer und Überweisungsbetrag) an dem Kartenleser, Bestätigung der Eingabe mit O.K.
– Überprüfung der Transaktionsdaten durch Sie auf dem Display des Lesers

Das hohe Sicherheitsniveau von Sm@rtTAN plus wird letztlich in Verbindung mit der Kontrolle der Daten durch Sie erzielt.

Fazit: eine sichere Lösung, die bei richtiger Anwendung und Kontrolle verlässlich gegen Missbrauch schützt.

Zeitgemäßer Komfort, innovative Sicherheit

Sm@rtTAN optic

Jede manuelle Dateneingabe stellt eine potenzielle Fehlerquelle beim Online-Banking dar. Hier setzt Sm@rtTAN optic an, die aktuelle Weiterentwicklung des innovativen Verfahrens Sm@rtTAN plus; Sm@rtTAN optic schaltet noch einmal ein Sicherheitsrisiko/ Verarbeitungsproblem aus; durch das Einlesen von Daten über eine optische Schnittstelle. Sie geben also die erforderlichen Informationen nicht manuell ein, sondern halten einen speziellen Kartenleser, den Sie von uns erhalten, vor eine animierte Grafik. Hierüber werden dann die Daten auf den Kartenleser übertragen – mit dem Ergebnis: noch mehr Sicherheit plus ein Maximum an Komfort für Sie.

Der Ablauf aus Ihrer Sicht:

– Erfassung der Überweisungsdaten im Online-Banking
– Nach dem Klick auf »Ausführen« erscheint die optische Schnittstelle. Diese Lichtsignale übertragen alle wichtigen Daten an das Lesegerät.
– Die Chipkarte (BankCard) in das Lesegerät stecken.
– Anschließend die F-Taste drücken und das Gerät mit dem Rücken genau vor die Grafik zur Monitoroberfläche halten. Wichtig: Die Pfeile von Lesegerät und optischer Schnittstelle sollten genau übereinander liegen.
– Im Display des Lesegeräts werden jetzt nacheinander alle wichtigen Daten angezeigt: die Art des Geschäftsvorfalls, die Empfängerkontonummer und der Betrag.
– Diese Daten sind mit dem Originalbeleg (z. B. der Rechnung) bzw. Ihren eingegebenen Daten zu vergleichen.
– Jetzt wird die nur für diese Transaktion gültige TAN angezeigt. Diese TAN muss jetzt von Ihnen im Online-Banking eingegeben werden, um die Transaktion auszuführen.

Übrigens: Die Daten können auch per Hand ein gegeben werden. Dazu einfach die TAN-Taste drücken und den Anweisungen im Online-Banking folgen. (analog Sm@rtTAN plus)

Schnell, flexibel und sicher: *mit EBICS für Firmenkunden*

Vor allem der sogenannte **E**lectronic **B**anking **I**nternet **C**ommunication Standard, **k**urz EBICS, bildet die Basis, um Firmenkunden neue Sicherheit und Flexibilität bei der Abwicklung des Zahlungsverkehrs zu bieten. Dabei verläuft die Kommunikation zwischen Bank und Kunde über die Anbindung des Firmenkunden ans Internet durch gesicherte Verbindungen. Die heute kostengünstig verfügbaren Übertragungsgeschwindigkeiten, ein Mehrfaches im Vergleich zum herkömmlichen ISDN, können ohne Einschränkung der Sicherheit genutzt werden. Sie benötigen lediglich ein aktuelles Zahlungsverkehrsprogramm wie z. B. windata professional 8, um die Vorteile von EBICS nutzen zu können.

Sichere Datenübertragung mit EBICS

Aktuelle Sicherheitsanforderungen werden sowohl auf der Ebene des Datentransports als auch auf Anwendungsebene erfüllt und sogar übertroffen.

– Die Datenübertragung erfolgt auf Basis einer TLS-Verschlüsselung unter Einsatz von zertifikatsbasierten gesicherten Servern.
– Authentizität, Integrität und Verbindlichkeit werden erzielt durch:
– Authentifikationssignatur
– Datenverschlüsselung
– Elektronische Unterschriften

Die verwendeten Schlüssellängen und die kryptographischen Verfahren entsprechen aktuellen und auch zukünftigen Anforderungen (A005-/A006- Signaturen mit bis zu 4.096 Bit). So sind in EBICS-Signaturverfahren besondere Schlüssellängen nutzbar, die für eine komplexe Verschlüsselung sorgen.

Umfassende Informationen
Schwarz auf weiß und auch im Netz

Damit Sie sich selbst intensiv mit dem Thema »Sicherheit im Online-Banking« vertraut machen können, bieten wir Ihnen zahlreiche Informationsunterlagen an. Detailierte Informationen und Broschüren finden Sie unter www.castell-bank.de unter »Konten & Online«.

– Sonderbedingungen Online-Banking

– Sicherheit im Online-Banking

– Bedienungsanleitung TAN-Generator

Gerne können Sie auch mit unseren Experten für Eletronic-Banking unter der kostenfreien Hotline 0800 1774 777 sprechen.

Fürstlich Castell'sche Bank,
Credit-Casse AG
Marktplatz 1
97070 Würzburg

Telefon 0800 1774 777
Telefax 0931 3083-998080
eb@castell-bank.de
www.castell-bank.de