Ergänzende Angaben zu einem „Betrugsvorfall beim Online-Banking“ als Anlage zur Strafanzeige der Polizei sowie Bearbeitungsgrundlage für das Geldinstitut

Vorgangsnummer:

Straftatbestände:

- **§ 263 a StGB Computerbetrug (PKS 517500)**
  in Verbindung mit
- § 202 a StGB Ausspähen von Daten
- § 303 b StGB Computersabotage
- § 303 a StGB Datenveränderung
- § 202 a StGB Ausspähen von Daten
- § 261 StGB Geldwäsche

1. Angaben zum Betroffenen

Name:	
Vorname:	
Geburtsdatum/-ort:	
Straße:	
PLZ Wohnort:	
Tel.-Nr.:	
E-Mail-Adresse:	

gibt an, Geschädigter eines Betruges beim Online-Banking geworden zu sein und teilt folgendes mit:

2. Hardware/Software/Internet

Für das Online-Banking benutzte ich ein/-en ☐ PC ☐ Notebook ☐ Smartphone
☐ Sonstiges:

Der **Zugang zum Internet** wird hergestellt über ein/-en
☐ DSL-Anschluss ☐ Standardmodem/ISDN ☐ Kabelanschluss ☐ Internetstick ☐ Smartphone
☐ Andere:

Mein **Internetprovider** ist
☐ Deutsche Telekom ☐ Vodafone ☐ Kabel Deutschland ☐ O2 ☐ E-Plus
☐ Andere:

Als **Betriebssystem** ist installiert
☐ Windows XP ☐ Windows Vista ☐ Windows 7 ☐ Windows 8 (8.1) ☐ Windows 10 ☐ iOS
☐ Version
☐ Andere

Aktualisiert wird das Betriebssystem
☐ automatisch
☐ manuell
☐ unbekannt

Das für die Transaktion/-en benutzte Benutzerkonto des PC hatte
☐ Administratorrechte ☐ einfache Benutzerrechte ☐ Gastrechte ☐ unbekannt

Eine **Antivirensoftware** ist ☐ installiert ☐ nicht installiert
Diese ist ☐ kostenpflichtig ☐ kostenfrei
☐ welche ?

Eine Aktualisierung der Antivirensoftware erfolgt
☐ automatisch ☐ durch Programm ☐ durch Betriebssystem
☐ manuell
☐ unbekannt

Datum/Zeit der letzten Aktualisierung:

Datum/Zeit letzten vollständigen Prüfung durch den Virenscanner:

Eine **Firewall** ist ☐ installiert diese ist ☐ aktiviert ☐ deaktiviert

Eine Aktualisierung der Firewall erfolgt
☐ automatisch ☐ durch Programm ☐ durch Betriebssystem
☐ manuell
☐ unbekannt

3. Online Banking

Folgende/s eigene Konto/-en wurden von der Phishing-Attacke betroffen:

IBAN	BIC	Name der Bank	Ort

Ich betreibe das Online-Banking und benutze folgendes Verfahren:

☐ PIN/TAN (Transaktionsnummern (TAN) auf der Liste sind nicht durchnummeriert)
☐ iTAN (Indizierte Transaktionsnummern, TAN auf der Liste sind durchnummeriert)
☐ mTAN/SMS-TAN (mobile TAN, wird von Bank auf Handy des Kunden gesendet)
☐ eTAN (elektron. TAN, Kunde hat TAN-Generator, der elektron. eine TAN erzeugt)
☐ eTAN Plus (wie eTAN, zusätzlich Einbindung von Überweisungsdaten)
☐ HBCI/FinTS (Chipkarte und Lesegrät, USB am PC, wie EC Karte mit PIN)
☐ Andere

☐ Ich benutze eine Banking-Software (z.B WiSo-Money/MeinGeld/Starmoney/Handy-App o.a.)

☐ welche ?

Ich benutze keine Banking-Software sondern habe die Internetseite der Bank aufgerufen, indem ich

☐ meinen Webbrowser gestartet und die Internetadresse in die Browserzeile eingegeben habe

☐ das im Favoriten-Ordner oder Lesezeichen-Symbol gespeicherte Lesezeichen der Internetadresse der Bank angeklickt habe

☐ auf einen Link einer E-Mail der Bank geklickt habe

☐ Sonstiges

Ich bin

☐ erstmalig

☐ wiederholt

Opfer eines Betruges im Onlinebanking geworden.

4. Dateneingabe im vorliegenden Fall

Die Online-Banking-Sitzung habe ich am gegen Uhr begonnen.

☐ Ich erhielt einen Hinweis auf eine Sicherheitsabfrage

☐ Die Daten auf der Bildschirmmaske waren bereits eingetragen

☐ Ich erhielt einen Hinweis auf eine Fehlüberweisung, welche zurück gebucht werden sollte

☐ Während der Sitzung öffnete sich ein weiteres Fenster mit sinngemäß folgendem Inhalt:

☐ Während des Überweisungsvorgangs öffnete sich kein weiteres Fenster

☐ Ich habe folgende Daten in die Online-Maske der Internetseite eingetragen:

☐ Kontonummer

☐ PIN

☐ TAN

☐ Sonstiges

5. Verhalten des PC

Nach Eingabe der Daten verhielt sich mein PC/Notebook/Smartphone folgendermaßen:

☐ Überweisungsvorgang wurde unterbrochen

☐ Überweisungsvorgang wurde nicht unterbrochen

☐ PC „stürzte ab“ ☐ PC lief normal weiter

☐ Ich erhielt einen Hinweis auf eine Sicherheitsabfrage

☐ Ich erhielt einen Hinweis auf eine Rücküberweisung

☐ Sonstiges

Ich habe ☐ einen ☐ keinen Suchlauf durch das Antiviren-Programm unternommen.
Das Antiviren-Programm hat ☐ eine Schadsoftware ☐ keine Schadsoftware festgestellt.
Ich habe nach dem Vorfall das Betriebssystem ☐ neu aufgesetzt ☐ nicht verändert.

Ein Virenreport/Trojanerreport
☐ liegt bei
☐ wird nachgereicht

6. Überweisungsdaten

Nach Einblick in die Umsatzliste des Kontos habe ich festgestellt, dass folgender Betrag/folgende Beträge missbräuchlich von meinem Konto abgebucht wurde/n:

Nr.	Datum (TT.MM.JJ)	Betrag	IBAN	BIC	Name Empfänger

Der Betrag zu Nr. _____ konnte durch die Bank wieder zurück gebucht werden.
Der Betrag zu Nr. _____ wurde durch die Bank in Höhe von _____ € entschädigt.

7. Datensicherung

Ich bin damit einverstanden, dass durch die Polizei eine Kopie der Festplatte meines PC/Notebook für weitere Ermittlungen erstellt wird
☐ Ja
☐ Nein

8. Sonstige Vermerke

9. Anlagen

☐ Kontobelege ☐ Überweisungsbeleg der Onlineüberweisung ☐ keine
☐ Andere
☐ Virenreport

10. Ermächtigung für die Datenanforderung beim Kreditinstitut des geschädigten Kontoinhabers

Ich/wir erklären uns damit einverstanden, dass mein/unser Kreditinstitut gegenüber den Ermittlungsbehörden die erforderlichen Auskünfte zu den angezeigten Transaktionen erteilt.

Polizeiliche Vorgangsnummer	
Kontoinhaber	
Kreditinstitut	
IBAN	
BIC	

Datum	Sachbearbeitende Dienststelle	Unterschrift Geschädigter/Kontoinhaber

Bearbeitungsnummer des Kreditinstitutes:

Hinweis für den Sachbearbeiter des Kreditinstitutes:
Es wird gebeten, Daten welche dem Kreditinstitut im Zusammenhang mit dem angezeigten Sachverhalt vorliegen,

> Transaktionsdatum/-Uhrzeit
> Betrag
> Zielkonto (IBAN/BIC)
> Name des Zielkontoinhabers
> Verwendungszweck der Transaktion
> Rückruf der Transaktion (Ja/Nein)
> Rückruf der Transaktion erfolgreich (Ja/Nein)

so schnell wie möglich an die sachbearbeitende Polizeidienststelle zu übersenden.

WICHTIGER HINWEIS FÜR DEN ANZEIGENERSTATTER:
Ursache für diese widerrechtliche Abbuchung ist ein heimlich eingeschleustes Schadprogramm auf Ihrem genutzten PC/Notebook oder Smartphone. Sorgen Sie zuerst für eine gründliche Überprüfung des Gerätes, bevor sie damit wieder Zugangsdaten im Internet nutzen!
Wichtige Informationen und eine Anleitung, wie Sie ihren genutzten PC/Notebook oder Smartphone säubern, erhalten Sie in dem Informationsblatt „Achtung! Schadprogramm!“, welches Sie auf den Internetseiten des „Ratgeber Internetkriminalität“

www.polizei-praevention.de

finden.
Auch wenn die Transaktion von ihrem Konto nicht erfolgt ist, liegt eine strafbare Handlung vor. Erstatten sie auch in diesem Fall unbedingt Anzeige. Beachten sie bitte auch in diesem Fall die Hinweise aus dem Merkblatt „Achtung! Schadprogramm!“.

HINWEIS FÜR POLIZEI UND GELDINSTITUT:
Der Fragebogen wurde durch das Landeskriminalamt Niedersachsen entworfen, um die Datenqualität bei der Bearbeitung dieser Delikte zu verbessern und soll sowohl der Polizei als auch den Geldinstituten als Vorgangsgrundlage zur Verfügung stehen.
Er kann bundesweit genutzt werden und ist auf den Internetseiten des „Ratgeber Internetkriminalität“

www.polizei-praevention.de

zur Verwendung hinterlegt. Dort findet man auch weitere hilfreiche Tipps, um sich vor Cyberkriminalität zu schützen.

POLIZEI
NIEDERSACHSEN

Herausgeber:
Landeskriminalamt Niedersachsen, Zentralstelle Cybercrime, Am Waterlooplatz 11, 30169 Hannover

Stand: Januar 2015