LKA Niedersachsen

Landeskriminalamt Niedersachsen

Zentralstelle Prävention und Jugendsachen
Am Waterlooplatz 11
30169 Hannover
Tel.: 0511 26262-3203

praevention@lka.polizei.niedersachsen.de
www.lka.niedersachsen.de
www.polizei-beratung.de

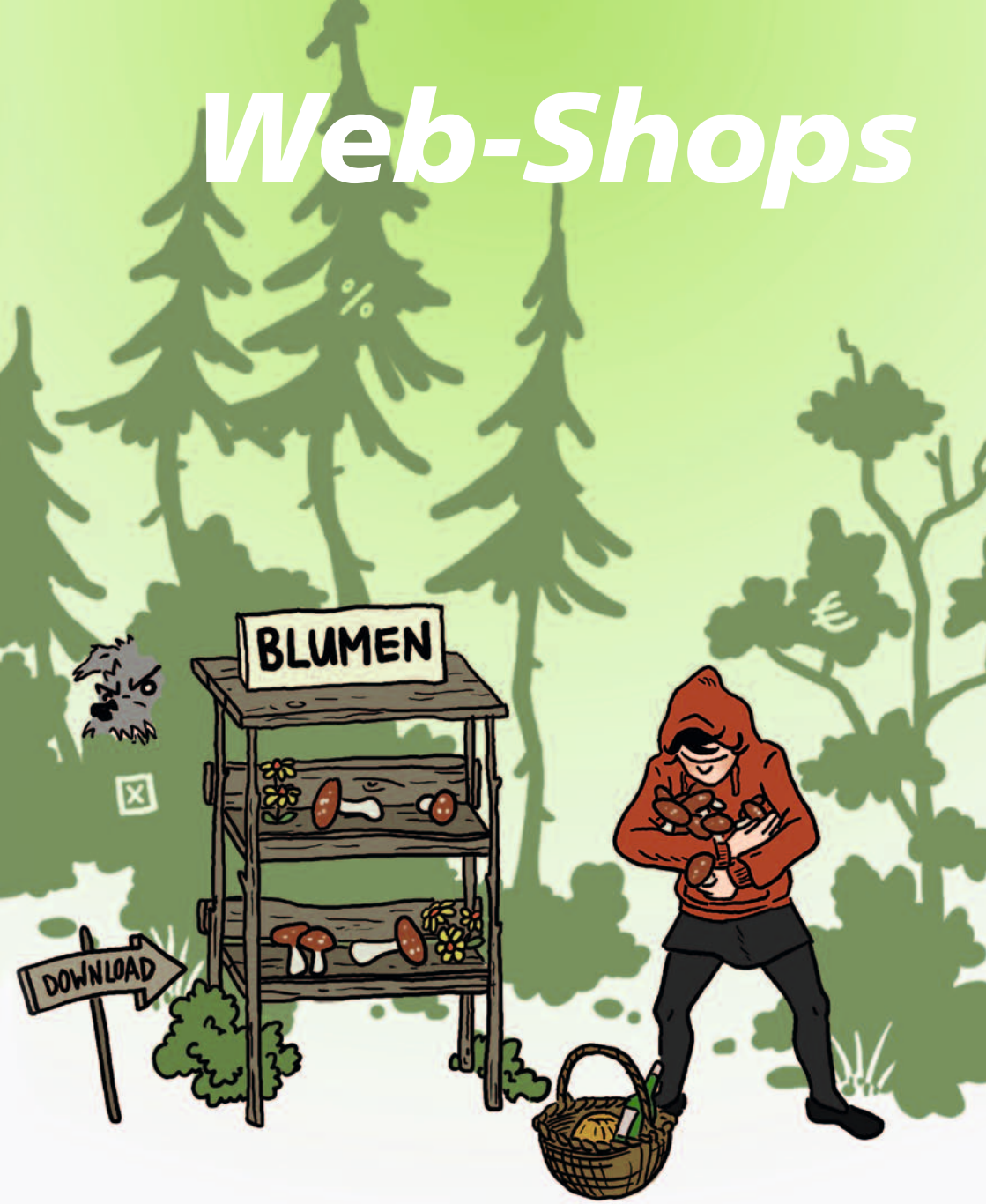
LASSEN SIE SICH KEINE MÄRCHEN AUFTISCHEN

Das Präventionsprogramm des Landeskriminalamtes Niedersachsen

gegen Internetkriminalität

LKA Niedersachsen

Web-Shops



LKA Niedersachsen

THEMA Internetkriminalität

…und die Moral von der Geschicht…

Fake-Shops
to fake (englisch): fälschen, imitieren

Neben den seriösen Web-Shops gibt es auch unseriöse Angebote, sogenannte „Fake-Shops“.
Beim Betrug mit „Fake-Shops“ handelt es sich um das Abändern einer bekannten, real existierenden Domain eines Webshops sowie dem Einstellen ins Web unter ähnlicher Aufmachung.

Es werden z. B. hochwertige Elektroartikel günstiger offeriert und potenzielle Käufer können Ware gegen Vorkasse bestellen. Das Produkt wird aber nicht geliefert.

Schutz vor Fake-Shops im Web

- Stellen Sie einen persönlichen Kontakt zum Anbieter her.
- Sehen Sie das Impressum ein.
- Werden Sie misstrauisch, wenn der Kontakt ausschließlich über E-Mail erfolgen kann.
- Nutzen Sie Bezahldienste.
- Hinweis: Eine Anzeige bei der Polizei ist auch online möglich: www. polizei.niedersachsen.de

Achtung:
Oftmals werden Domainendungen mit „.com“, „.net“, „.info“ und „.de“ für die „Fake-Shops“ missbraucht. Bei Endungen die auf „.de“ lauten, besteht die Möglichkeit der Abfrage über „Denic“. Hier ist stets die letzte Aktualisierung zu beachten.

Soziale Netzwerke

LKA Niedersachsen

THEMA Internetkriminalität

...und die Moral von der Geschicht...

Soziale Netzwerke erfreuen sich steigender Beliebtheit. Immer mehr Menschen pflegen ihre Kontakte oder Hobbys über das Internet und stellen dort persönliche Informationen ein. Die virtuelle Welt birgt jedoch Gefahren für den leichtfertigen Nutzer. Wenn Sie die nachfolgenden Tipps beherzigen, können Sie die Gefahren minimieren und sich vor bösen Überraschungen schützen.

Schutz vor Missbrauch in virtuellen Netzwerken

- Machen Sie sich mit den Datenschutzbestimmungen und den Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen sozialen Netzwerkes vertraut.
- Legen Sie ein Profil erst dann an, wenn Sie wissen, was mit Ihren Daten geschieht, wer darauf Zugriff hat und ob diese Daten eventuell weitergegeben werden.
- Klären Sie, wer die Rechte an hochgeladenen Bildern hält (z. B. Party-Bilder für Online-Alben) und ob der Netzwerkbetreiber diese weiter verwenden darf.
- Stellen Sie generell keine heiklen Bilder ein.
- Überlegen Sie genau, welche Informationen Sie für wen freigeben möchten.
- Stellen Sie keine vertraulichen Informationen über Freunde oder Arbeitgeber ins Netz. Sie könnten nicht nur einen Freund sondern auch Ihre Arbeitsstelle verlieren.
- Wählen Sie Ihre Kontakte mit Bedacht und überprüfen Sie, ob die Person tatsächlich zu den Freunden hinzugefügt werden soll.
- Klicken Sie nicht auf Links, die Sie per E-Mail erhalten, denn soziale Netzwerke werden bevorzugt für Identitätsdiebstahl oder Phishing benutzt.
- Achten Sie auf Ihr Passwort. Nutzen Sie unterschiedliche, sichere Passwörter, die Sie regelmäßig ändern sollten.

Hinweise:
Nutzen Sie die Möglichkeiten des Netzwerkes und geben Informationen nur für Freunde frei, die Sie auch wirklich kennen. Da z. B. Spammer Profile mit Ihrem Namen anlegen und Nachrichten an Ihre Freunde senden, sollten Sie Ihre Freundesliste nicht öffentlich schalten.

Unbekannte können durchaus „böse“ Absichten haben. Kriminelle erforschen auf diesem Wege gern die Lebensgewohnheiten von potenziellen Opfern. Daher ist es für die Kommunikation mit Unbekannten empfehlenswert, sich eine zusätzliche E-Mail Adresse bei einem Free-Mailer anzulegen.

Betrügerische Seiten verstecken sich oft hinter einer sogenannten Kurz-URL, bei der ein Nutzer die tatsächliche Zieladresse nicht erkennen kann. Hier werden dann z. B. Nutzername und Kennwort abgefragt und an Kriminelle weitergeleitet.

Alles, was Sie in sozialen Netzwerken veröffentlichen, lässt sich anschließend nicht mehr löschen und bleibt für immer im Netz. Verlinkungen, Kommentare auf fremden Profilen oder Beiträge in Foren können kaum noch entfernt werden und bleiben auch bestehen, wenn Sie Ihr Profil löschen. Das heißt im Klartext: Das Internet vergisst nichts!

Phishing

LKA Niedersachsen

THEMA Internetkriminalität

…und die Moral von der Geschicht…

Mit dem Begriff „Phishing“ („Passwort und Fishing“) wird das Abgreifen von persönlichen Online-Zugangsdaten über z. B. gefälschte E-Mails, falsche www.-Adressen usw. bezeichnet.

Die Zugangsdaten für Ihre Online-Accounts (z. B. Online-Banking, E-Mail, Online-Auktionshäuser, Online-Bezahldienste usw.) sowie Kreditkartendaten sind ständig gefährdet und bei den Internet-Tätern sehr begehrt. Diese nutzen Ihre Accounts für die vielfältigen Betrugshandlungen – und Sie müssen sich möglicherweise mit Regressforderungen von Geschädigten auseinandersetzen!

Schutz vor Phishing

- Machen Sie Ihren PC „sicher“, bevor Sie im Internet surfen (Mappeninnenseite).
- Öffnen Sie nie E-Mail-Anhänge oder Dateianhänge in Messenger- und Chat-Diensten von unbekannten oder nicht erwarteten Nachrichten.
- Verwenden Sie für Bankgeschäfte nie einen Link, der per E-Mail übersandt wurde.
- Wenn Sie die Internetseite Ihrer Bank oder andere sensible Seiten aufrufen, geben Sie immer manuell die Adresse in die Adresszeile Ihres Browsers ein.
- Achten Sie darauf, dass die Verbindung zu Ihrer Bank in der Adresszeile mit https:// beginnt (sichere Verbindung).
- Achten Sie darauf, dass bei einer zertifizierten sicheren Verbindung in der unteren Browserleiste ein Schloss angezeigt wird.
- Informieren Sie sich über die verschiedenen Verfahren zum sicheren Durchführen von Online-Banking (z. B. HBCI, SMS-TAN usw.).

Hinweise

Eine Bank wird nie Ihre persönlichen Zugangsdaten, persönliche Identifikationsnummer (PIN) oder Transaktionsnummern (TAN) per E-Mail erfragen! Im Zweifelsfall sprechen Sie persönlich mit Ihrer Bank. Auch andere seriöse Verkaufsplattformen, Bezahlsysteme usw. erfragen Ihre persönlichen Zugangsdaten nie außerhalb des Geschäftsvorganges.

Erstatten Sie sofort Strafanzeige bei Ihrer Polizeidienststelle, wenn Ihre Daten missbräuchlich genutzt wurden. Jede Minute ist wichtig!!!

Informieren Sie sofort Ihre Bank oder den jeweiligen Dienstanbieter, um weiteren Schaden zu vermeiden.

Ändern Sie sofort, sofern Sie noch Zugang haben, die Passwörter der betroffenen Accounts.

Sichere Passwörter

LKA Niedersachsen

THEMA Internetkriminalität

...und die Moral von der Geschicht...

Passwortschutz fängt bei Ihnen zu Hause an. Sie selbst können dazu beitragen, Ihr System und Ihre privaten Daten vor Unbefugten zu schützen. Sie lassen ja auch nicht jeden in Ihre Wohnung, oder? Verhindern Sie den Diebstahl, die Veränderung und den Missbrauch Ihrer Daten.

Nachfolgend ein paar Regeln, die Ihnen die Erstellung von sicheren Passwörtern und deren Umgang erleichtern sollen:

Geheime Passwörter

Geben Sie Ihre Passwörter nicht an Freunde, Bekannte oder Fremde weiter. Bewahren Sie Passwörter verdeckt auf und nicht an Orten wie der Pinnwand oder am Monitor. Speichern Sie auch nicht die Passwörter im Computer (z. B. im Browser, in Textdateien oder Tabellen).

Zeichenmix

Verwenden Sie keine bekannten Wörter, Namen und Zahlenkombinationen. Tier- und Spitznamen, Geburtsdaten und Vergleichbares sind tabu! Nutzen Sie scheinbar unvorhersehbare Kombinationen aus Buchstaben, Zeichen, Sonderzeichen, Zahlen. Verwenden Sie z. B. die Anfangsbuchstaben einer Liedzeile mit Satzzeichen und ergänzen diese um weitere Sonderzeichen und Zahlen. Ersetzen Sie auch Buchstaben durch Zahlen (z. B. „3“ für „E“). Aus der Liedzeile „Ein Männlein steht im Walde ganz still und stumm, Es hat von lauter Purpur ein Mäntlein um.“ wird z. B. das Passwort „EMsiWgsus,3hvlPeMu.“ (Dieses Beispiel nicht verwenden.) Verwenden Sie diese Methode auch bei der Beantwortung von Sicherheitsfragen, die diverse Dienste als zweiten Schutz vorgeben.

Unterschiedliche Passwörter / kein Passwortrecycling

Verwenden Sie für jeden Zugang ein neues sicheres Passwort und niemals dasselbe. Benutzen Sie keine alten Passwörter erneut. Bedenken Sie auch Verbindungen von z. B. Mailaccount zu Shoppingaccount, wobei oft die Mailadresse schon der Nutzername ist.

Voreingestellte Passwörter ändern

Voreingestellte Passwörter dienen lediglich zum ersten Schutz. Diese stehen jedoch oft in Handbüchern, auf Klebeetiketten am Gerät oder Sie haben diese per Mail erhalten. Fremde können diese Daten ablesen oder abgefangen haben, möglicherweise sind diese sogar noch im Mailpostfach unter den Mails abgelegt. Denken Sie daran, sämtliche Hardware (Internetrouter/DSL-Modem/Repeater/Powerline), sowie die Datenübertragung (z. B. Wlan) mit sicheren Passwörtern zu versehen.

Gewinnversprechen / Gewinnmitteilungen (per Telefon)

Bei Gewinnversprechen und Gewinnmitteilungen am Telefon wird der Kauf eines hochwertigen PKW oder Bargeld in Aussicht gestellt.
Die Täter geben sich als Rechtsanwälte, Notare oder als ähnlich seriös wirkende Berufsstände aus. Sie erklären, dass der Angerufene bei einer Auslosung gewonnen habe. Der Gewinn könne jedoch nur gegen eine Überweisungs- oder Verwaltungsgebühr, die meist an andere Personen ins Ausland transferiert werden soll, eingelöst werden. Tatsächlich ist jedoch eine Gewinnübergabe nie vorgesehen.
Die Anrufe erfolgen von einem ausländischen Callcenter unter Nutzung der „Voice over IP-Nummer“ (VoIP). Diese erscheint im Display des Angerufenen als deutsche Festnetznummer.

Schutz vor falschen Telefonversprechen

- Überlegen Sie genau, ob Sie tatsächlich an dem Preisausschreiben teilgenommen haben. Kein Unternehmer hat etwas zu verschenken.
- Legen Sie sofort auf.
- Leisten Sie keine Vorauszahlungen.
- Informieren Sie die nächste Polizeidienststelle.

Hinweis:
Vorsicht ist immer dann geboten, wenn Bedingungen an die Auszahlung des Gewinns geknüpft werden. Überweisen Sie z. B. vorab keine Verwaltungsgebühren.

Betrug

LKA Niedersachsen

THEMA Internetkriminalität

... und die Moral von der Geschicht ...

Abmahnbetrug / Abofalle

Auf Internetseiten wie „www.XXX-downloaden.de“ bieten die Betreiber vermeintlich kostenlose Computerprogramme zum Download an. Vor Beginn des Downloads wird aufgefordert, die eigenen persönlichen Daten einzutragen. Der Nutzer wird unbewusst zum Abschluss eines kostenpflichtigen Abos verleitet, zumeist für die Dauer von mindestens einem Jahr. Die Geschädigten erklären bei der späteren Anzeigeerstattung, dass auf den Seiten kein Hinweis auf die Kosten vorhanden war.

Vom Oberlandesgericht Frankfurt wurde aktuell in einem Fall des Abmahnbetruges festgestellt, dass Angebote mit versteckten Kostenhinweisen als gewerbsmäßiger Betrug zu werten sind (Az.: 1 Ws 29/09).

Hinweise

- Überprüfen Sie nach Erhalt der Rechnung, ob ein Kostenhinweis vorhanden war und ob dieser unzulänglich formuliert wurde.
- Bestreiten Sie ggf. den Vertragsabschluss, da ein unerwarteter oder versteckter Kostenhinweis unwirksam sein kann.
- Fragen Sie auch bei der Verbraucherzentrale nach und nehmen Sie eine Rechtsberatung in Anspruch.

Wenn auf der Webseite ein Hinweis auf Kostenpflichtigkeit sofort erkennbar ist, wäre ein Betrug zu verneinen. Stößt man auf diesen Hinweis jedoch erst durch Blättern (Scrollen) auf der Internetseite, muss aufgrund des Urteils von einem Betrug ausgegangen werden.

Ebay-Betrug

Beim Ebay-Betrug gibt es zahlreiche Varianten wie beispielsweise den Täuschungs- oder Verpackungstrick, bei dem der Ersteigerer durch Hinweise wie „Geboten wird nur auf eine Verpackung“ z. B. über ein angebotenes Handy oder Notebook getäuscht wird.

Eine weitere Variante ist der Dreiecksbetrug:
Die Täter gelangen an die Daten anderer Ebay-Nutzer, deren Accounts sie zuvor, beispielsweise mit Hilfe von „Phishing-Mails“, „gehackt“ hatten. In den Mails wird ein vermeintliches Problem mit dem Account vorgetäuscht und zur Eingabe der persönlichen Daten aufgefordert. Unter Nutzung der fremden Daten wird dann reger Handel betrieben. Dabei können die Täter sowohl Waren erhalten, die sie auf fremden Namen bestellt haben, aber auch Waren verkaufen, die sie gar nicht besitzen.

Schutz vor Ebay-Betrug

- Seien Sie vorsichtig bei Bargeld-Anweisungen.
- Geben Sie besonders Acht bei Handelspartnern im Ausland.
- Geben Sie grundsätzlich keine Bankdaten heraus.
- Nehmen Sie die Bezahlung des Gegenstandes über PayPal oder andere Bezahldienste vor.

Betrug im KFZ-Sektor

Die Täter akzeptieren sofort den Preis eines im Internet angebotenen PKW, LKW oder eines Motorrads. Sie übersenden einen gefälschten Scheck, der einen überhöhten Betrag ausweist. Anschließend bitten sie, den Scheck einzulösen und den Differenzbetrag mittels des Bargeldtransfers ins Ausland zurück zu überweisen.

Bei der Überprüfung der Schecks in der Bank – eine mehrwöchige Prüfungsdauer ist im Auslandszahlungsverkehr gebräuchlich – stellt sich heraus, dass der Scheck wertlos ist.

Schutz vor KFZ-Betrug

- Wenn Sie merken, dass Sie betrogen wurden, machen Sie Ihre Überweisung rückgängig und nehmen Sie sofort Kontakt zu Ihrer Bank auf.
- Wenn Sie einen Bargeldtransfer durchgeführt haben, bei dem Sie betrogen wurden, nehmen Sie sofort Kontakt zu dem Geldtransfer-Dienstleister auf und lassen die Transaktion stoppen. Solange noch keine Auszahlung erfolgt ist, wird die Summe grundsätzlich zurück überwiesen.
- Wenn das Geld bereits abgerufen ist, setzen Sie sich mit der Online-Fahrzeugbörse in Verbindung und bitten um sofortiges Löschen des Inserates.
- Erstatten Sie Strafanzeige bei der Polizei.

Hinweis:
Weitere wertvolle Tipps sind bei den bekannten Automobilclubs erhältlich.

So schützen Sie Ihren PC und Ihre Daten

Damit sowohl Ihr Computer als auch Ihre Daten optimal gesichert sind, empfehlen wir Ihnen die Berücksichtigung folgender Hinweise:

Schutz für die Technik

Aktuelles Betriebssystem
- Schalten Sie automatische Updates ein. Ältere Systeme werden durch die Hersteller nicht mehr gepflegt.

Firewall
- Schalten Sie die Firewall des Betriebssystems ein.

Oder
- Setzen Sie eine spezielle Firewall-Software ein.

Antivirenprogramm
- Installieren Sie regelmäßig die aktuelle Version.
- Schalten Sie regelmäßige Aktualisierungen der Virensignaturen ein.

Hinweis:
Kostenpflichtige Antivirenprogramme werden zumeist häufiger aktualisiert und bieten weitergehende Schutzmechanismen.

Browser und genutzte Programme
- Aktualisieren Sie regelmäßig Ihren Browser.
- Konfigurieren Sie Browsereinstellungen, z. B. PopUp.

Blocker
- Binden Sie Zusatzprogramme im Browser ein (z. B. Anzeige der fremden IP, Meldung inkriminierter Seiten etc.).

WLAN
- Nutzen Sie Verschlüsselungsmöglichkeiten des Routers.
- Ändern Sie das voreingestellte Standard-passwort.

Schutz für die Daten

- Gehen Sie verantwortungsbewusst mit persönlichen Daten um.
- Speichern Sie möglichst keine persönlichen Daten und Kennwörter auf dem PC.
- Folgen Sie keinen Links aus E-Mails etc., wenn diese im Rahmen von Käufen, Verkäufen, Bankgeschäften übermittelt wurden. Geben Sie die URL immer direkt ein.
- Öffnen Sie keine Mails von unbekannter Herkunft. Fragen Sie beim Versender nach oder löschen Sie die Mail im Zweifel.

Hinweise:
Vermeintliche Gewinnspiele und Gratisangebote haben in vielen Fällen nur den Zweck, die persönlichen Daten der Nutzer zur erlangen.

Banken und „Geschäftspartner" erfragen grundsätzlich keine Daten wie Kennworte, Transaktionsnummern und Zugangsdaten.

Führen Sie die Datensicherung regelmäßig durch.