Shoppen, Musik herunterladen, Spielen – so surfen Jugendliche sicher durchs Netz

Eine Welt ohne Internet? Gar nicht vorstellbar. Informieren, einkaufen, austauschen – alles läuft online. Wenn es allerdings ums Geld geht, ist Vorsicht angebracht. Wichtige Tipps.

Onlineshopping

Bewusst einkaufen

Beim Onlineshopping sind Bücher, Schuhe oder coole Accessoires viel schneller eingekauft als im Laden. Drei bis vier Klicks und die neuen Sneakers sind bestellt. Genau das kann aber auch zu voreiligen und vielleicht unnötigen Käufen verleiten. Am besten also im Vorfeld gut überlegen, ob man die Sachen wirklich braucht, sie sich leisten kann UND Taschengeld oder Joblohn wirklich dafür ausgeben will. Auch ein Preisvergleich vor dem Bestellklick hat Sinn.

Verkaufsbedingungen

Wer im Internet etwas veräußert, muss seine Verkaufsbedingungen angeben. Das geschieht über die Allgemeinen Geschäftsbedingungen, kurz AGB. In der Regel müssen Käufer vor der Bestellung per Klick bestätigen, dass sie sie gelesen haben. Die Texte sind allerdings kompliziert. Am besten, Jugendliche holen sich beim Übersetzen die Hilfe ihrer Eltern.

Kauf widerrufen

Wer die georderten Sachen doch nicht haben möchte, wem sie nicht gefallen oder passen, der kann seinen Internetkauf in der Regel binnen 14 Tagen ohne Angabe von Gründen schriftlich widerrufen. Ein formloses Schreiben per Brief oder Mail an den Verkäufer genügt (Versandbestätigung am besten aufbewahren!). Natürlich muss man die Sachen auch zurückschicken.
In Ausnahmefällen ist das Widerrufsrecht ausgeschlossen. Das gilt vor allem, wenn man etwas bei Privatleuten bestellt, also zum Beispiel bei Ebay oder Ebay Kleinanzeigen. Oder wenn man individuell angefertigte Produkte ordert, z. B. ein mit Namen bedrucktes T-Shirt oder eine Tasse mit dem eigenen Foto.

Bei seriösen Shops einkaufen

Seriöse Shops erkennen Onlinekäufer unter anderem daran, dass der Anbieter seine Kaufbedingungen von vornherein klarstellt, die AGB und Datenschutzregeln leicht auf der Homepage zu finden und klare Lieferfristen und Versandbedingungen angegeben sind. Auch Gütesiegel für Onlineshops liefern Anhaltspunkte dafür, ob man mit vertrauensvollen Verkäufern zu tun hat. Dazu zählen etwa die Siegel „Safer Shopping“, „EHI Geprüfter OnlineShop“ oder „Trusted Shops“. (Mehr Infos dazu, siehe Linkliste.)

Auf Verschlüsselung achten

Sensible Daten zur eigenen Person oder im Rahmen der Bezahlung immer nur auf Internetseiten mit sicherer Verbindung eingeben. In der Browser-Zeile sollte ein goldenes Schloss-Symbol erscheinen und die Internetseite in der Browser-Zeile mit „https“ beginnen, nicht nur mit http. Das „s“ bedeutet ein Extra an Sicherheit.

Gut mit Passwörtern umgehen

Bei vielen Shops müssen die Käufer einen eigenen Account für ihre Bestellungen anlegen. Dazu legen sie ein Passwort fest. Hier gilt:

1. Am besten immer für jeden Shop ein eigenes Passwort festlegen.
2. Die Passwörter sollten aus Ziffern, Klein- und Großbuchstaben sowie Sonderzeichen bestehen.
3. Die Passwörter niemals von Computer oder Smartphone automatisch für eine Seite speichern lassen, sondern immer wieder neu eingeben. Man weiß nie, wer die Geräte in die Hände bekommt.

Bezahlen im Internet

Verschiedene Möglichkeiten stehen zur Auswahl:

- Bezahlen auf Rechnung: Das ist einer der sichersten Wege. Der Verkäufer schickt die Ware und legt seine Rechnung bei. Die begleicht der Käufer dann am einfachsten per OnlineBanking.
- Lastschriftverfahren: Dieses können Jugendliche nutzen, die bereits ein eigenes Girokonto haben (siehe hierzu auch Checkliste „Budget im Griff“). Sie erteilen dem Shopbetreiber eine einmalige Einwilligung, dass er den Preis von diesem Konto abbuchen kann. Wer das nutzt, sollte sein Konto gut im Blick behalten. Bucht jemand etwas zu Unrecht oder zu viel ab, lässt sich die Lastschrift nämlich noch widerrufen. Man hat aber nur acht Wochen ab der Abbuchung dazu Zeit.
- Paydirekt: Das ist ein sehr sicherer Onlinebezahldienst, den die deutschen Banken, also auch die PSD Bank München, anbieten. Wer ihn nutzen möchte, muss sich einmalig dafür bei seiner Bank registrieren (weitere Infos, siehe Links unten).
- giropay: Für diese sichere Bezahlvariante brauchen Jugendliche ebenfalls ein eigenes Girokonto. Sie wählen giropay beim Bezahlvorgang aus, geben dann die Bankleitzahl ein und werden anschließend zur Online-Banking-Seite der eigenen Bank geleitet. Dort melden sie sich mit ihrer PIN-Nummer an und finden ein bereits passend ausgefülltes Überweisungsformular. Einmal alles prüfen und schließlich mit einer TAN (Transaktionsnummer) die Überweisung bestätigen (weitere Infos, siehe Links unten).
- Kreditkarte: Jugendliche, die zum Beispiel die Prepaidkarte PSD BasicCard haben, können auch damit im Internet bezahlen. Wichtig: Sie müssen vorher sicherstellen, dass der Kaufbetrag auch wirklich auf der Karte geladen ist. Überziehen dürfen sie nicht.
- Nachnahme: Hierbei zahlt der Käufer beim Postboten, der das Paket bringt. Nachteil: Das kostet zusätzliche Gebühren.
- Vorkasse: Diese Variante braucht viel Vertrauen. Erst, wenn der Käufer nämlich gezahlt hat, schickt der Verkäufer die Ware los. Kauft man bei Privatleuten, zum Beispiel über Ebay, ist Vorkasse allerdings die Regel.

Downloads/Apps

Kostenloses Herunterladen von Filmen oder Musik

Auch, wenn das noch so verlockend ist – hier müssen Jugendliche ganz vorsichtig sein. Schneller als gedacht, ist das Urheberrecht der Komponisten oder Filmemacher verletzt und das kann richtig teuer werden. Auf Nummer sicher gehen Familien, die Streamingdienste wie Spotify, Deezer, Juke, Napster oder Amazon Video nutzen.

Finger weg von Musik- oder Filmtauschbörsen

Hier wird es ganz riskant. Oft laden die Nutzer die Dateien bei solchen Tauschbörsen nämlich nicht nur herunter, sondern stellen sie gleichzeitig anderen Nutzern zum Download zur Verfügung. Das nennt man Filesharing und das ist verboten, wenn der Urheber nicht ganz ausdrücklich zugestimmt hat. Wichtig: Der Bundesgerichtshof hat hierzu einerseits entschieden, dass Eltern für das illegale Filesharing der eigenen Kinder nicht haften, wenn sie sie darüber belehrt und eine Teilnahme verboten haben (Az. I ZR 74/12). Haben sie aber konkrete Anhaltspunkte dafür, dass die Kinder ihren Internetanschluss rechtsverletzend nutzen, müssen sie den Computer überprüfen oder dem Kind den Zugang zum Internet teilweise versperren. In einem zweiten Verfahren haben die Richter geurteilt, dass Eltern zwar nicht verpflichtet sind, ihre Kinder zu verraten. Geben sie in einem Schadenersatz-Prozess den Namen aber nicht preis, kann das dazu führen, dass sie als Anschlussinhaber selbst für die verletzten Urheberrechte geradestehen müssen (Az. I ZR 19/16). Auch der Europäische Gerichtshof hat Ende 2018 geurteilt, dass Inhaber eines Internetanschlusses generell für Urheberrechtsverstöße haften, die von ihrem Anschluss begangen wurden. Sie können sich nicht allein dadurch befreien, dass auch andere Familienmitglieder Zugriff hatten (Az. C-149/17; Links zu den Urteilen, siehe unten).

Vorsicht bei kostenlosen Angeboten

Gratis-Apps oder kostenfreie Angebote im Netz sind vielversprechend, können aber auch gefährlich für das Portmonee werden. Oft verbergen sich dahinter Kostenfallen. Die Anbieter wollen etwa mit besonders toll erscheinenden Lockangeboten eigentlich zum Kauf teurerer Produkte verleiten, oder der Nutzer schließt ohne es zu merken ein Abo ab. Sehr häufig ist der Absender auch darauf aus, Daten zu sammeln.

Achtung Gratis-Apps

Viele Apps sind erst einmal kostenlos. Dennoch kann die Handyrechnung plötzlich in die Höhe schnellen, weil sich der Nutzer beim Spielen zum Beispiel dazu verleiten lässt, zusätzliche Gimmicks, Figuren oder Upgrades zu kaufen. Das nennt man In-App-Käufe. Tipp: Auf vielen Smartphones lässt sich vorab einstellen, dass solche Einkäufe automatisch blockiert werden.

Sichere Apps herunterladen

Viele App-Anbieter sind auf die Daten der Nutzer aus. Sie wollen sie zum Beispiel an Unternehmen verkaufen, die dann gezieltere Werbung schalten können. Vorsicht ist daher geboten, wenn man Daten angeben soll, die für die App-Nutzung gar nicht erforderlich sind. Das ist beispielweise der Fall, wenn man den Zugriff auf das komplette Adressbuch erlauben soll. Generell sollte man eine App zudem immer nur aus dem offiziellen Store (z. B. Google Play oder App Store) runterladen und auch bei Updates immer darauf achten, ob sich die Zugriffsrechte vielleicht geändert haben.

Achtung Phishing

Was ist Phishing?

Dahinter verbirgt sich eine der größten Gefahren für alle, die im Internet einkaufen oder Online-Banking nutzen. Betrüger versuchen, mittels gefälschter E-Mails und Webseiten, die täuschend echt aussehen, an die Passwörter oder Bankdaten – Geheimnummern, TANs, Kontonummer, Kreditkartennummer – heranzukommen. Als seriöse Bank oder Internetshop getarnt fordern sie den Empfänger zum Beispiel in einer E-Mail auf, seine Daten zu aktualisieren, Zugangsdaten zum OnlineBanking oder Passwörter für Shops anzugeben. So etwas würde eine Bank niemals machen! Ausgestattet mit den Geheimdaten geht der Betrüger nun auf Kosten seines Opfers auf Shoppingtour oder räumt dessen Konto leer.

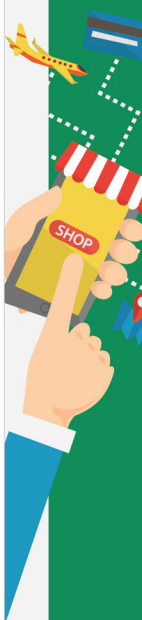
Woran erkenne ich eine Phishing Mail?

Wenn Jugendliche die folgenden Sachen beobachten, müssen sie ganz vorsichtig sein:

- ✓ Der Absender fragt in seiner Mail nach vertraulichen Daten wie Passwörtern, PINs, TANs und anderen Informationen zu der Kontoverbindung.
- ✓ Die E-Mails sind im HTML-Code geschrieben. Das erkennt man daran, dass der Text der E-Mail mit verschiedenen Schriftarten und Schriftgrößen formatiert wird, Bilder (z. B. Logos) verwendet werden und/oder der Hintergrund eine andere Farbe hat.
- ✓ Der angegebene Link wirkt auf den ersten Blick echt, auf den zweiten erkennt man jedoch ungewöhnliche oder falsch geschriebene Bestandteile der Internetadresse.
- ✓ In der E-Mail finden sich Grammatik- und Rechtschreibfehler.
- ✓ In der Mail weisen zum Beispiel Banken oder große Onlinekaufhäuser darauf hin, dass sich das Abrechnungssystem geändert hat oder Software-Updates erfolgt sind. Das ist ein deutliches Phishing-Warnsignal.
- ✓ Oftmals kommt die E-Mail auch von einer komischen Absenderadresse oder wird in Kopie (= in CC) an zahlreiche weitere Empfänger geschickt.
- ✓ Die E-Mail ist nicht in der üblichen landestypischen Sprache der Bank geschrieben.
- ✓ Die E-Mail verwendet eine nicht-personalisierte Anrede wie "Sehr geehrte Damen und Herren".

Wie schütze ich mich vor Phishing?

- ✓ Links aus solch verdächtigen Mails niemals anklicken und erst recht keine Dateianhänge öffnen.
- ✓ Stattdessen mit den Eltern über die Mail reden. Sie können z. B. die Bank, die in der Mail als Absender auftaucht, informieren.
- ✓ Die Firewall am eigenen Rechner sollte immer auf dem neusten Stand sein.
- ✓ Niemals über öffentlich zugängliche Rechner, z. B. im Internetcafé, ins OnlineBanking gehen.
- ✓ Das eigene Konto immer gut im Blick haben, um falsche Abbuchungen schnell zu entdecken. Weitere Tipps: Siehe Links unten.



Und wenn die Falle schon zugeschnappt hat?

- ✓ Haben Jugendliche Kontobewegungen entdeckt, die sie nicht selbst veranlasst haben, oder doch versehentlich ihre Daten preisgegeben, sollten sie direkt mit ihren Eltern reden.
- ✓ So schnell wie möglich die Bank informieren, um Konto oder Kreditkarte sperren zu lassen. Außerhalb der Geschäftszeiten zum Sperren der Karte und des Online-Zugangs einfach den Sperr-Notruf wählen: 116 116. Hat ein Onlineshop für etwas Geld abgebucht, das man nicht gekauft hat, am besten auch den Account dort löschen oder die Zugangsdaten sofort ändern.
- ✓ Unberechtigte Lastschriften lassen sich noch bis zu acht Wochen später rückgängig machen.
- ✓ Generell gilt: Wurde Geld zu Unrecht abgebucht, sollte immer auch Anzeige bei der Polizei erstattet werden.

Linktipps

Die Seite der Verbraucherzentrale NRW gibt Jugendlichen Tipps rund um das Thema Onlineshopping:
www.checked4you.de/onlineshopping

Hier können Jugendliche einen Test zum Thema Onlineshopping machen:
www.checked4you.de/extras/quizspiele/wie-fit-bist-du-im-online-shopping-351104

So erkennt man seriöse Shops:
initiatived21.de, internet-guetesiegel.de

Das Bundesamt für Sicherheit informiert über Sicherheit beim Onlineshopping:
www.bsi-fuer-buerger.de > digitale Gesellschaft > Einkaufen im Internet

Was ist Paydirekt und wie funktioniert es?
www.paydirekt.de

Infos zu giropay:
www.psd-muenchen.de/giropay

Urteile des BGH und des EuGH zum Thema Haftung der Eltern bei Filesharing im Volltext:
www.juris.bundesgerichtshof.de; curia.europa.eu

Die EU-Initiative für mehr Sicherheit im Netz erklärt, wie man das eigene Smartphone sicher macht:
www.klicksafe.de/smartphones

Sicherheitstipps rund um das Thema Apps:
www.klicksafe.de/apps

Was ist Phishing und wie schützt man sich davor?
www.bsi-fuer-buerger.de > Risiken > Spam, Phishing & Co

Antworten etwa zum Thema illegale Downloads oder Betrug im Internet:
www.klicksafe.de > Rechtsfragen im Netz > iRights

Wenn man seine PSD girocard oder BasisCard sperren lassen muss:
www.sperr-notruf.de

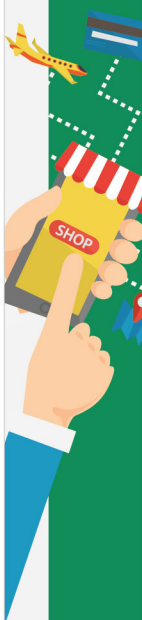
Das Jugendkonto der PSD Bank München im Überblick:
www.psd-muenchen.de/girostart

Infos rund um die aufladbare Kreditkarte der PSD Bank München:
www.psd-muenchen.de/prepaid

Tipps, wie ein sicheres Passwort aussehen kann:
praxistipps.chip.de/was-ist-ein-sicheres-passwort-die-besten-tipps_3482

Sicherheitstipps fürs OnlineBanking:
www.psd-muenchen.de/Sicherheit-im-OnlineBanking

Die Informationen für unsere Checkliste sind das Ergebnis sorgfältiger Recherchen und wurden mehrfach kontrolliert. Dennoch übernehmen wir keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der in dieser Checkliste veröffentlichten Informationen.



Stand 01/2019