

Richtlinien zur Bewirtschaftung der Schulbudgets

1. Allgemeines

Die Bestimmungen der Gemeindeordnung für das Land Nordrhein-Westfalen (GO) und der Gemeindehaushaltsverordnung NRW (GemHVO) sowie die für die Stadt Bergisch Gladbach geltenden Dienstanweisungen gelten uneingeschränkt.

Die städtischen Schulen erhalten Mittel aus dem Ergebnis- und Finanzhaushalt für den pädagogischen Betrieb zur eigenverantwortlichen Bewirtschaftung zur Verfügung gestellt (Schulbudget).

Die Schulen verwalten und bewirtschaften diese Mittel direkt über das bei der Bensberger Bank/VR-Bank eingerichtete Girokonto (Schulgirokonto). Das Konto wird auf Guthabenbasis geführt; eine Überziehung ist nicht möglich.

2. Berechnung, Umfang und Zuweisung des Schulbudgets

Das jeweilige Budget wird der Schule nach einem festgelegten Verteilerschlüssel unter Berücksichtigung der Schülerzahlen nach amtlicher Schulstatistik und eines Sockelbetrages zugewiesen; Haupt- und Förderschulen erhalten einen Zuschlag. Die Auszahlung des Schulbudgets erfolgt in zwei Jahresraten jeweils zum 01.02. und 01.09. eines Jahres durch Überweisung auf das Schulgirokonto. Haushaltsmittel für die Beschaffung von Lernmitteln nach dem Lernmittelfreiheitsgesetz erhalten die Schulen in einer Summe zum 01.06 eines Jahres auf das Schulgirokonto überwiesen.

Die Höhe des Budgets und damit der Raten richtet sich nach dem jährlich zur Bewirtschaftung freigegebenen Gesamtansatz. Eventuelle Änderungen bereits budgetierter Finanzmittel wird den Schulen umgehend mitgeteilt, in jedem Fall frühzeitig vor Beginn eines Haushaltsjahres.

Zusammensetzung, inhaltliche Ausgestaltung und Verwendung der Budgetansätze für das Produkt 003.400.020 „Ausstattung von Schulen“ innerhalb der Produktgruppe 003.400 „Schulträgeraufgaben“ ergeben sich aus nachstehender Übersicht:

Sach-konto	Bezeichnung	Inhalte
5235000 / 7235000	Unterhaltung Betriebsvorrichtung	Aufwand für Reparaturen von Mobiliar und Geräten etc. / Neu- und Ersatzbeschaffungen.
5240000 / 7240000	Verwaltungs-/ Betriebsaufwand	Aufwand für Lehr- und Sachmittel, Schulwanderungen, Schulveranstaltungen, Schülervertretung, Untersuchungskosten etc
5430000 / 7430000	Geschäftsaufwendungen	Bürobedarf, Telefongebühren, Internetgebühren, GEZ, Kopier-/Umdruckpapier, Kopien etc.
5242000 / 7242000	Lernmittel	Kosten der Lernmittelfreiheit
I-Auftrag 40028001	Investition bewegliche Sachen	Ersatz- und Neubeschaffungen von Geräten, Ausstattungsgegenständen, Mobiliar

3. Mittelverwendung

Über die Verwendung des Schulbudgets entscheidet die Schulkonferenz nach § 59 (7) Schulgesetz im Rahmen des von der Stadt Bergisch Gladbach (Schulverwaltung) festgelegten Verwendungszwecks. Zur Vorbereitung der notwendigen Beschlüsse ist es ratsam, einen schulinternen Wirtschaftsplan aufzustellen.

Die Vorschriften der Übergangswirtschaft gem. § 82 GO NRW sind auch von den Schulen zu beachten.

Bei der Verplanung des Budgets ist darauf zu achten, dass die laufenden Sachkosten über das ganze Haushaltsjahr abgedeckt werden können.

Die Mittel sind wirtschaftlich und sparsam einzusetzen. Die Schulleiterinnen und Schulleiter sind dafür verantwortlich, dass Verbindlichkeiten nur im Rahmen der zur Verfügung gestellten Haushaltsmittel eingegangen, die zugewiesenen Mittel zweckentsprechend verwendet und alle Nachweise vollständig und richtig geführt werden.

4. Verfügungsberechtigung

Die Stadtkasse erteilt der Bensberger Bank / VR-Bank gegenüber Vollmacht, dass jeweils bis zu sechs Personen berechtigt sind, im Rahmen des Guthabens über das Konto zu verfügen: Die gemeinsame Verfügungsberechtigung (jeweils zwei Bevollmächtigte gemeinsam) wird auf einer besonderen Unterschriftenkarte zum Konto festgelegt.

Die Trennung zwischen Anordnungsbefugnis und Kassengeschäft muss gewährleistet sein.

Der/die Zeichnende für die Anordnungsbefugnis darf nicht identisch sein mit dem/der Zeichnenden für die sachliche und rechnerische Richtigkeit (Vier-Augen-Prinzip)

Neben den Schulleiterinnen und Schulleitern und deren Stellvertreterinnen und Stellvertretern sollte im Vertretungsfall mindestens auch eine Schulsekretärin und/oder Lehrkraft zeichnungsberechtigt sein.

Unterschriftsvollmachten werden von der Stadtkasse erteilt und bei der Bensberger Bank / VR-Bank hinterlegt. Durchschriften verbleiben bei der Schule, der Schulverwaltung und dem Rechnungsprüfungsamt.

5. Auftragserteilung

Zuständig für die Vergabe von Aufträgen sind grundsätzlich die Schulleiterinnen und Schulleiter. Bei Abwesenheit ist der/die ständige Vertreter/in zeichnungsberechtigt.

Mit Zustimmung der Schulverwaltung können die Schulleiterinnen und die Schulleiter die Zeichnungsberechtigung für die Erteilung von Aufträgen auf die Stellvertreterinnen und Stellvertreter, weitere Schulleitungsmitglieder und die Schulsekretärin als Daueraufgabe übertragen.

Die Bestellgrenze für Schulleiterinnen und Schulleiter liegt bei 2.500.-- €.

Die Vorschriften zu Ziffer 3.4 der Vergabeordnung der Stadt Bergisch Gladbach (VergO) über die freihändige Vergabe von Aufträgen sind analog von den Schulen anzuwenden. Danach ist eine formlose Preisermittlung bei möglichst 4 Firmen, die aktenkundig zu machen ist, vorzunehmen.

Sofern für einen Auftrag (unabhängig von der Anzahl der Gegenstände) oder eine Dienstleistung die festgelegte Höchstgrenze überschritten wird, ist für die Auftragserteilung die Schulverwaltung zuständig.

Eine Stückelung von Aufträgen mit dem Ziel die Höchstgrenze nicht zu überschreiten ist unzulässig.

Aufträge mit einem Wert von über 250.-- € sind grundsätzlich nur schriftlich unter Verwendung des städtischen Bestellscheinvordrucks und unter dem amtlichen Namen der Schule zu erteilen.

6. Abwicklung des Zahlungsverkehrs

Verantwortlich für die Abwicklung des Zahlungsverkehrs ist die jeweilige Schulleiterin oder der jeweilige Schulleiter.

Der Zahlungsverkehr der Schule ist grundsätzlich bargeldlos über das Schulgirokonto abzuwickeln. Näheres regelt die Dienstanweisung zur Bewirtschaftung des Schulbudgets und der Abwicklung des Zahlungsverkehrs über Girokonten für die Schulen der Stadt Bergisch Gladbach.

7. Abrechnung

Zur Überwachung und Kontrolle des Schulbudgets ist ein Einnahme- und Ausgabennachweis zu führen.

Alle Einnahmen und Ausgaben sind ordnungsgemäß zu belegen . Die Belege sind fortlaufend zu nummerieren und in dieser Ordnung abzuheften.

Die Ausgabebelege sind von dem zahlungsberechtigten Personenkreis sachlich und rechnerisch zu prüfen. Diese Prüfung ist durch das Abhaken der Einzelposition und des Gesamtbetrages oder in anderer geeigneter Form kenntlich zu machen.

Als Ausgabebelege gelten Originalrechnungen, Kassenzettel, Verwendungsnachweise usw. Sie sind mit dem Sichtvermerk der Schulleiterin bzw. des Schulleiters und dem Eingangsdatum zu vermerken und müssen Zeitpunkt sowie Art und Umfang der Leistung deutlich erkennen lassen.

8. Zahlungsvermerk

Alle Ausgabebelege müssen den Zahlungsvermerk (Stempel) enthalten:

Richtig geliefert/ausgeführt

Datum:

Unterschrift:

Der Rechnungsbetrag in Höhe von ____ € wurde amangewiesen

Datum:

Unterschrift:

9. Aufbewahrungsfristen der Belege und Kontengegenblätter

Die Aufbewahrungsfrist für Buchungsbelege, Bankkontoauszüge und Kontengegenblätter beträgt 10 Jahre (vgl. § 257 HGB). Die Frist beginnt mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung im Kontengegenblatt gemacht, der Kassenabschluss aufgestellt sowie geprüft wurde.

10. Sicherheit und Haftung

Die Schulleiterin bzw. der Schulleiter ist verantwortlich für die Einhaltung der Sicherheitsvorschriften und hat entsprechende Regelungen dazu in der Schule zu treffen.

Alle relevanten Schulgirounterlagen und Vordrucke, Berechtigungskarte für Kontoauszüge, EC-Karten, PIN-Nummern, Belege, Kontengegenblätter und sonstige Unterlagen sind unter Verschluss aufzubewahren und gegen Einbruch, Diebstahl und Feuer zu schützen.

Schadensfälle/Verluste sind unverzüglich vorab telefonisch der Schulverwaltung zu melden. Gleichzeitig ist das Schulgirokonto umgehend durch die Schule sperren zu lassen. Bei grob fahrlässigem Verhalten oder bei Verstößen behält sich die Schulverwaltung vor, die Schulleiterin bzw. den Schulleiter in Haftung zu nehmen

11. Kassenabschlüsse

Kassenabschlüsse erfolgen unterjährig am Ende eines jeden Quartals und zusätzlich zum Schluss des Kalenderjahres. Die notwendigen Formvorschriften werden von der Schulverwaltung in Abstimmung mit dem Rechnungsprüfungsamt vorgegeben. Näheres regelt die Dienstanweisung zur Bewirtschaftung der Schulbudgets und der Abwicklung des Zahlungsverkehrs über Girokonten für die Schulen der Stadt Bergisch Gladbach.

12. Nichtverwendete Mittel / Einsparungen

Die am Ende des Haushaltsjahres nicht in Anspruch genommenen Mittel des Schulbudgets (Einsparungen) stehen für entsprechende Ausgaben im nächsten Haushaltsjahr zu Verfügung, sofern dem nicht die Vorschriften des Haushaltsrechts entgegenstehen.

13. Überwachung und Prüfung der Kassengeschäfte

Mindestens einmal jährlich wird die ordnungsgemäße Führung der Kassengeschäfte, insbesondere die lückenlose Aufbewahrung der Kassenbelege, durch Prüfungen überwacht.

14. Inkrafttreten

Nach diesen Richtlinien ist ab dem 01.01.2011 zu verfahren.

Bergisch Gladbach, den 01.09.2010

Dienstanweisung zur Bewirtschaftung der Schulbudgets und der Abwicklung des Zahlungsverkehrs über Girokonten für die Schulen der Stadt Bergisch Gladbach

1. Allgemeines

Nach den im Oktober 2010 vom Rat beschlossenen Richtlinien zur Bewirtschaftung der Schulbudgets (Budgetierungsrichtlinien) erhalten die städtischen Schulen Mittel aus dem städtischen Haushalt zur eigenverantwortlichen Bewirtschaftung (Schulbudget).

Die Schulen verwalten und bewirtschaften diese Mittel selbstständig und eigenverantwortlich über ein städtisches Schulgirokonto.

Diese Dienstanweisung regelt die ordnungsgemäße Führung der Kassengeschäfte der Schulen im Sinne der beschlossenen Budgetierungsrichtlinien (siehe Anlage 1 der Dienstanweisung) und des Neuen Kommunalen Finanzmanagement (NKF).

2. Mittelverwendung

Die Mittel des Schuletats gliedern sich in drei Ein/Ausgabearten und sind nach den Vorgaben zweckgebunden zu verwenden für:

- „laufende Sachkosten“
- „Kosten der Lernmittelfreiheit“
- „Erwerb von Vermögensgegenständen“

Eingesparte Mittel bei den „Kosten der Lernmittelfreiheit“ dürfen für „laufende Sachausgaben“ verwandt werden. Umgekehrt gilt das gleiche.

Eingesparte Mittel für den „Erwerb von Vermögensgegenständen“ dürfen nicht für „Kosten der Lernmittelfreiheit“ oder „laufende Sachkosten“ verwandt werden. Umgekehrt gilt das gleiche.

Für Planung und Ausführung gilt folgender Hinweis: Neu- und Ersatzbeschaffungen von selbstständig nutzbaren Gegenständen mit einem Einzelwert unter 60,00 € (netto) = 71,40 € (brutto) werden als Aufwand unter „laufende Sachausgaben“ verplant und

verbucht. Neu und Ersatzbeschaffungen von selbstständig nutzbaren Gegenständen über 60,00 € netto (71,40 € brutto) sind als „Erwerb von Vermögensgegenständen“ zu verplanen und zu verbuchen.

Berechtigt zur Bewirtschaftung der Haushaltsmittel sind die Schulleiterinnen und Schulleiter, im Verhinderungsfall ihre Vertretungen im Amt.

Vor der Rechtskraft des städtischen Haushaltes, dürfen nur Auszahlungen geleistet werden, zu denen die Schule rechtlich verpflichtet ist oder die notwendig sind, um den Schulbetrieb aufrecht zu erhalten. Die Schulen werden über die Rechtskraft des Haushaltes informiert.

Sofern Zweifel über die freie Verfügbarkeit der Mittel bestehen ist im Einzelfall vor Auftragsvergabe die Einwilligung der Schulverwaltung einzuholen.

Zur Überwachung und Kontrolle des Geldverkehrs ist ein Nachweis nach den Vorgaben der Schulverwaltung und wie unter Punkt 5.1 beschrieben zu führen.

3. Schulgirokonto, Verfügungsberechtigungen, Barkassen

3.1 Schulgirokonto

Die Stadtkasse richtet für jede Schule ein neues Geschäftskonto (Schulgirokonto) bei der Bensberger Bank oder der VR-Bank ein, über das die Mittel des Schulbudgets und eventuelle andere öffentliche Drittmittel verwaltet werden.

Ein Unterkonto zu dem neuen Schulkonto (z. B. Spar/Festgeldkonto) ist auf Ebene der einzelnen Schule nur in Abstimmung mit der Schulverwaltung zulässig. Soweit die Schule bisher solche Konten unterhält sind diese der Schulverwaltung zu melden und Bestände gegebenenfalls dem Schulgirokonto zuzuführen.

3.2 Verfügungsberechtigung

Zur Verfügung des Schulkontos und zur Unterschriftsleistung sind nur die Personen berechtigt, denen die Stadtkasse die Unterschriftsvollmacht erteilt hat und die bei der jeweiligen kontoführenden Bank hinterlegt sind.

Einzelheiten zur Hinterlegung und Änderungen notwendiger Unterschriftsvollmachten der Verfügungsberechtigten sind mit der Schulverwaltung abzustimmen.

3.3 Barkassen

Bisherige Barkassen sind aufzulösen. Noch vorhandene Restguthaben sind dem Schulgirokonto zuzuführen und als Einnahme zu verbuchen. Zu Prüfungszwecken ist die Auflösung der Barkasse der Schulverwaltung anzuzeigen. Diese behält sich eine sofortige Kassenprüfung vor.

4. **Zahlungsverkehr und Internet-Banking**

4.1 Zahlungsverkehr

Verantwortlich für die Abwicklung des Zahlungsverkehrs nach § 94 GO sind die Schulleiterinnen und Schulleiter

Der Zahlungsverkehr ist grundsätzlich bargeldlos und nach wirtschaftlichen Gesichtspunkten über das Schulgirokonto abzuwickeln.

Bei der Rechnungsabwicklung sind Zahlungsfristen einzuhalten und mögliche Skonto- und Rabattgewährungen sowie sonstige Preisvergünstigungen in Anspruch zu nehmen.

Mit der Feststellung der sachlichen und rechnerischen Richtigkeit wird die Verantwortung für die Richtigkeit der im Rechnungsbeleg enthaltenen und die die Zahlung maßgebenden Angaben sowie für die Einhaltung der Grundsätze der Sparsamkeit und Wirtschaftlichkeit übernommen. Ferner wird bestätigt, dass die Lieferung oder Leistung entsprechend der Bestellung oder des Auftrags erfolgte.

Die Erteilung von Bankeinzugsermächtigungen durch die Schulleiterinnen und Schulleiter ist zulässig, sofern die Verbindlichkeit nur im Rahmen der zur Verfügung stehenden Haushaltsmittel eingegangen wird. Von Dritten vorgenommene Abbuchungen sind unverzüglich auf ihre Richtigkeit und Rechtmäßigkeit zu überprüfen.

Für wiederkehrende Zahlungsverpflichtungen dürfen im Rahmen der zur Verfügung stehenden Haushaltsmittel und nur auf ein Haushaltsjahr bezogen durch die Schulleiterinnen und Schulleiter Daueraufträge eingerichtet werden.

Die Ausstellung von Kreditkarten für das Schulgirokonto ist nicht zulässig.

Zeichnungsberechtigte, die bereits die sachliche und rechnerische Richtigkeit bescheinigt haben sind nicht mehr berechtigt als Bevollmächtigte bei Überweisungen mitzuwirken (siehe auch Ziffer 4 der Budgetierungsrichtlinien „Vier-Augen-Prinzip“). Bevollmächtigte dürfen bei Überweisungen auch nicht mitwirken wenn sie selbst oder deren Familienangehörige Zahlungsempfänger sind.

4.2 Internet-Banking

Die bargeldlose Abwicklung des Zahlungsverkehrs kann auch im Rahmen des Internet-Banking erfolgen, sofern die nachfolgenden Voraussetzungen vorliegen und das Basiswissen „Sicherheit im Online-Banking“, das den Schulleiterinnen und Schulleitern gegen Empfangsbestätigung ausgehändigt wird, beachtet wird:

- Der für das Internet-Banking verwendete Rechner muss über ein aktuelles Virenschutzprogramm und eine Firewall verfügen (Hinweis: Betriebssysteme wie Windows Vista und Windows 7 haben dieses standardmäßig, bei Windows XP ist eine zusätzliche Firewall zu installieren). Die Programme sind regelmäßig auf dem aktuellen Stand zu halten.
- vor Eingabe der TAN (Transaktionsnummer) ist der Empfängercode zu kontrollieren
- Bei Nutzung eines WLAN-Anschlusses (Drahtlos-Netzwerk) für das Internet-Banking muss eine sichere Verschlüsselung der Zugangsdaten zum Netzwerk gegeben sein.
- Die Verwendung einer Funktastatur beim Internet-Banking ist nicht gestattet.
- Alle mit dem Internet-Banking im Zusammenhang stehenden Unterlagen sind getrennt voneinander und sicher aufzubewahren, so dass sie unbefugten Personen nicht zugänglich sind (siehe auch Ziffer 10 der Budgetierungsrichtlinien).

Folgender Ablauf ist für das Internet-Banking vorgesehen:

Jede von der Stadtkasse bevollmächtigte Person erhält von der Bensberger Bank oder der VR-Bank Bergisch eine persönliche Identifikationsnummer (PIN) mit der ein Zugriff auf das Internet-Banking möglich wird.

Die für das Internet-Banking zugeteilte persönliche Identifikationsnummer (PIN) ist in regelmäßigen Abständen (mindestens alle 3 Monate) zu ändern und darf nicht im IT-System hinterlegt sein.

Gleichzeitig erhält jeder/jede Bevollmächtigte eine Bankcard und einen Taschenkartenleser zur Generierung von gültigen Transaktionsnummern (TAN).

Überweisungen vom Schulgirokonto können nur von zwei bevollmächtigten Personen gemeinsam abgewickelt werden. Die erste Person gibt die Überweisung unter ihrer eigenen PIN ein. Die so angelegte Überweisung muss dann von einer zweiten Person unter Verwendung der eigenen PIN zur Zahlung frei gegeben werden.

Kontoinformation (Kontostände, Umsätze etc.) können beide Zugangsberechtigte unabhängig voneinander und ohne Freigabe durch eine zweiten mit ihrer persönlichen PIN und der Bankcard abrufen.

Computerausdrucke von Überweisungen beim Internet-Banking sind als fest zu verbindende Bestandteile der Ausgabebelege zu verwahren. Sind diese nicht vorhanden sind entsprechende Überweisungsvermerke auf den Ausgabebelegen vorzunehmen. Als Beleg für die Kontobewegungen werden aber nur die Original-Kontoauszüge, die den Schulen von den vorgenannten Banken zur Verfügung gestellt werden, anerkannt.

5. Buchführung /Kassenabschlüsse/Aufbewahrungsfristen

5.1 Buchführung

Zur Überwachung und Kontrolle des Schulbudgets ist ein Einnahme- und Ausgabenachweis zu führen.

Alle Bankbewegungen (Ein-/Auszahlungen) müssen zeitnah chronologisch aufgezeichnet und nachvollziehbar belegt werden (siehe auch Ziffer 7 der Budgetierungsrichtlinien).

Der Nachweis der Bankbewegungen hat ausnahmslos durch Erfassung auf den von der Schulverwaltung als Exel-Datei (12 Arbeitsblätter Januar – Dezember) zur Verfügung gestellten Kontogegenblättern zu erfolgen (siehe Anlage 3). Manuelle Eintragungen in

einem ausgedruckten Kontogegenblatt (z.B. bei Systemausfall) sind unverzüglich nach zu erfassen.

Jeweils am Monatsende ist das Kontogegenblatt abzuschließen, auszudrucken und von den Verantwortlichen zu unterzeichnen. Anschließend wird das nächste Kontogegenblatt in der Excel-Datei aufgerufen und dort die Eintragungen des entsprechenden Monats vorgenommen.

Sofern eine Schule Gelder verwaltet, die nicht zum originären Schulbudget gehören (öffentliche Drittgelder wie z. B. Landeszuschüsse, zweckgebundene stg. Zuschüsse etc.) ist neben dem Erfassen jeder Kontenbewegung auf dem Kontogegenblatt gleichzeitig eine Erfassung auf einem zusätzlichen „Unterkontoblatt“ (siehe Anlage 4) erforderlich, auf dem diese speziellen Mittel nach ihrer Zweckbestimmung gesondert abgebildet werden.

Grundlage für die Eintragungen im Kontogegenblatt bilden die Ein-/Auszahlungsbelege. Diese sind unverzüglich in das jeweils für einen Monat geltende Kontogegenblatt einzutragen. Die Belege sind in der Reihenfolge ihrer Eintragung im Kontogegenblatt fortlaufend zu nummerieren und in dieser Ordnung zeitnah (mindestens einmal wöchentlich) abzuheften. Nachweise zu den Überweisungen (Durchschriften von Überweisungsträgern oder Ausdrücke der elektronischen Überweisung) sind den jeweiligen Kontoauszügen der Banken zuzuordnen und gemeinsam mit diesen zeitlich geordnet (Auszug-Nr./Blatt-Nr.) aufzubewahren. Auf den Kontoauszügen ist zu den einzelnen Buchungen die Beleg-Nummer zu vermerken.

Die Eintragungen im Kontogegenblatt sind bei jeder Kontenbewegung mit den Buchungen auf den Kontoauszügen der vorgenannten Banken abzustimmen. Abweichungen müssen sofort aufgeklärt werden. Nicht aufzuklärende Unstimmigkeiten sind der Schulverwaltung umgehend mitzuteilen.

5.2 Kassenabschlüsse

Kassenabschlüsse erfolgen unterjährig am Ende eines jeden Quartals und zusätzlich zum Schluss des Kalenderjahres.

Am Ende eines jeden Quartals (31.03./30.06./30.09/31.12.) ist ein Abschluss zu fertigen. Die entsprechenden Verwendungsnachweise (abgezeichnete Kontogegenblätter **und** Unterkontoblätter) sowie eine Kopie der Excel-Datei sind

jeweils bis zum 10. des Folgemonates an die Schulverwaltung zur weiteren Veranlassung abzugeben.

Mit der letzten Quartalsabrechnung zum 31.12. eines Jahres ist die Buchführung eines Haushaltsjahres abzuschließen. Die Gesamtabrechnung ist grundsätzlich und gleichzeitig im Rahmen eines Jahresabschlussberichts der Schulverwaltung gegenüber durch Darstellung der Kontostände (Kontoauszug der Bank) sowie einem Einnahme- und Ausgabenachweis in Papierform zu belegen. Die Schulleiterin oder der Schulleiter bescheinigt die Richtigkeit des Jahresabschlusses und legt die Gesamtjahresabrechnung der Schulverwaltung spätestens bis zum 10. Januar vor. Die notwendigen Formvorschriften werden von der Schulverwaltung in Abstimmung mit dem Rechnungsprüfungsamt vorgegeben.

Nach der Prüfung des Jahresabschlusses und der Feststellung der Ordnungsmäßigkeit durch die Schulverwaltung erfolgt eine schriftliche Entlastung der Schulleiterin oder des Schulleiters.

6. Nichtverwendete Mittel / Einsparungen

Die am Ende des Haushaltsjahres nicht in Anspruch genommenen Mittel des Schulbudgets (Einsparungen) stehen für entsprechende Ausgaben im nächsten Haushaltsjahr zu Verfügung, sofern dem nicht die Vorschriften des Haushaltsrechts entgegenstehen.

7 Überwachung und Prüfung der Schulbudgets und der Ein-/Auszahlungen

Mindestens einmal jährlich wird die ordnungsgemäße Führung der Kassengeschäfte, insbesondere die lückenlose Aufbewahrung der Kassenbelege, durch unvermutete Prüfungen von Mitarbeitern der Schulverwaltung überwacht, die nicht mit der Führung der Kassengeschäfte der Schulen beauftragt sind. Das Recht auf Prüfung des Rechnungsprüfungsamtes wird hierdurch nicht eingeschränkt.

8 Geltungsbereich

Diese Dienstanweisung gilt verbindlich für alle städtischen allgemein bildenden Schulen mit Ausnahme der städtischen Verbundschule. Die Bewirtschaftung des

Schulbudgets und Abwicklung des Zahlungsverkehrs der Verbundschule wird in einer gesonderten Dienstanweisung geregelt.

9. Inkrafttreten

Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft. Gleichzeitig verlieren die Verbindlichen Regelungen zur buchungstechnischen Umsetzung der Budgetierungsrichtlinien vom 11.12.2003 ihre Gültigkeit.

- Anlage 1: Budgetierungsrichtlinien vom 01.09.2010
- Anlage 2: Basiswissen „Sicherheit beim Online-Banking“
- Anlage 3: Muster „Kontogegenblatt“
- Anlage 4: Muster „Unterkontoblatt“



BASISWISSEN

Schutz vor Daten-Spionen

Online-Banking ist einfach und sicher. Dennoch: Damit Sie Ihr Geld vor dem Zugriff von Internet-Betrügern schützen, muss Ihr Computer frei sein von schädlichen Spionage-Programmen. Dieses Dokument erklärt Ihnen, worauf Sie achten und was Sie tun müssen.

Inhalt

Basiswissen	1
So funktionieren Phishing-Mails	2
So funktionieren Daten-Spione	3
Diese Hinweise sollten Sie beachten	5
So wählen Sie eine sichere Geheimzahl	7
Weitere Informationen im Internet	7



So funktionieren Phishing-Mails

Der Begriff „Phishing“ ist in aller Munde. Auch Sie haben vielleicht schon Phishing-Mails in Ihrem Posteingang gehabt, genauso wie unzählige andere Spam-Mails.

Spam-Mails sind unerwünschte E-Mails mit meist werblichem Charakter. Mails, die die Empfänger auffordern, geheime Kontodaten über das Internet preiszugeben, nennen Fachleute „Phishing-Mails“. Der Begriff „Phishing“ ist eine Kombination aus den englischen Wörtern „Password“ und „fishing“.

Phishing-Mails stammen von Betrügern

Die Betrüger fischen also online nach Passwörtern, um damit den Zugang zu fremden Konten zu erhalten. Die Absender verschicken diese Mails in der Regel massenhaft und weltweit von mehreren Computern aus, die sie zu ganzen Netzwerken (Bot-Netzen) zusammenfassen. Um diese Phishing-Mails unschädlich zu machen, gibt es eine wirksame Möglichkeit: Löschen Sie diese Mails sofort! Und bedenken Sie:

Ihre Bank bittet Sie weder per E-Mail noch telefonisch, Kontodaten wie PIN und TAN preiszugeben!

Wie Sie Phishing-Mails erkennen

Phishing-Mails gibt es in vielen Varianten. Eins haben sie aber gemeinsam: Sie nutzen Vorwände und gefälschte Absender-Adressen, Web-Seiten und Eingabe-Masken, die beispielsweise einer Banking-Anwendung täuschend ähnlich sehen. Hier einige Beispiele für Vorwände, die in Phishing-Mails oft auftauchen:

- Software oder Bankdaten sollen aktualisiert werden
- Phishing-Mails warnen selbst vor Phishing-Mails
- Sie erhalten eine Mahnung zum Beispiel für Ihre Telefon- oder GEZ-Rechnung
- Ihre Kreditkarte oder VR-BankCard ist abgelaufen
- Sie sollen Ihr Passwort erneuern
- Sie sollen Daten für Umfragen oder Gewinnspiele bestätigen

Ein typischer Beispielfall: Sie erhalten per E-Mail eine gefälschte Rechnung mit einer sehr hohen Forderung. Diese Mail enthält einen Link oder einen als PDF-Datei getarnten Anhang. Beim Ausführen installiert sich ein Spionage-Programm auf dem PC.

Viele Phishing-Seiten bestehen aus einer Eingabe-Maske, in die Sie sowohl Ihre Kontonummer als auch PIN und TAN eintippen sollen. Auf echten Banking-Seiten werden PIN und TAN immer auf nacheinander folgenden Seiten abgefragt.

Viele Phishing-Mails erkennen Sie daran, dass sie verhältnismäßig viele Rechtschreib- und Grammatikfehler enthalten. Seien Sie deshalb vorsichtig, wenn Sie in einer geschäftlichen E-Mail über schlechtes Deutsch stolpern.



Grundsätzlich können Sie erwarten, dass ein Unternehmen, bei dem Sie Kunde sind, Sie persönlich mit Ihrem Namen anredet. Nicht alle, aber die meisten Phishing-Mails beginnen mit unpersönlichen Anreden wie „Sehr geehrter Kunde“ oder ähnlichem.

Deswegen: Löschen Sie alle E-Mails, deren Herkunft Sie nicht genau kennen.

Unseriöse Job-Angebote

Ebenfalls in Form von E-Mails tauchen immer wieder Job-Angebote auf, in denen serlös anmutende Unternehmen den Empfängern anbieten, als Finanz-Makler tätig zu werden. Auch wenn Sie angeblich lukrative Provisionen einstreichen können, stellen Sie Ihr Konto nie für fremde Zahlungen zur Verfügung!

Oft handelt es sich um Gelder, die aus den Erträgen von Phishing-Mails stammen. Unter Umständen riskieren Sie Freiheitsstrafen wegen Geldwäsche und Schadenersatz-Ansprüche der geschädigten Bankkunden. Informieren Sie Ihre Bank und die Polizei, wenn Sie eine solche Mail erhalten.

Der Stornierungs-Trick

Ein anderer Trick funktioniert nach folgendem Muster: Betrüger bestellen per E-Mail Gebrauchtwagen oder andere Waren, oder sie buchen eine Ferienwohnung. Mit dem Anbieter vereinbaren sie, den Preis vorab zu überweisen. Dazu benutzen Sie allerdings ein fremdes, mittels Phishing ausgespähtes Konto. Unter einem Vorwand stornieren die Täter dann den Kauf – ebenfalls per E-Mail. Die bereits überwiesene Geldsumme soll das Opfer ins Ausland transferieren. Dass ihm angeblich wegen der entstandenen Unannehmlichkeiten ein Teilbetrag zugesprochen wird, ist ein Trick, um ihn in Sicherheit zu wiegen. Das Geld landet beim Täter oder der Tätergruppe.

Seien Sie deshalb vorsichtig, wenn Gutschriften auf Ihrem Konto erscheinen, die kurze Zeit später zurückgefordert werden – insbesondere bei Auslandstransfers. Informieren Sie im Zweifelsfall Ihre Bank oder die Polizei.

So funktionieren Daten-Spione

Ein technisch einwandfreier Computer ist die Grundvoraussetzung dafür, dass Sie Ihre Überweisungen sicher online erledigen können. Wenn Ihr Computer nicht ausreichend geschützt ist, können schädliche Computer-Programme, zum Beispiel so genannte Trojaner, unbemerkt auf Ihre Festplatte gelangen und dort die unterschiedlichsten Schäden anrichten.



So können Trojaner auf Ihren Computer gelangen:

- Eingebettet in scheinbar harmlosen Downloads
- Über Datenträger wie Diskette oder CD-ROM
- Versteckt als Datei-Anhang in einer Phishing-Mail (zum Beispiel mit dem Namen "Rechnung.pdf.exe")
- Durch Surfen auf einer manipulierten Internet-Seite

Antiviren-Software und Firewall sind Pflicht

Einige Trojaner sind so programmiert, dass sie beispielsweise die PIN/TAN-Eingabe beim Online-Banking manipulieren. Andere leiten den Nutzer auf eine gefälschte Internet-Seite.

Unerlässlich ist es deshalb, dass auf Ihrem Computer ein Antiviren-Programm sowie eine Firewall installiert sind, die Sie regelmäßig aktualisieren. Diese Programme können Trojaner und andere Viren identifizieren und löschen. Auch Ihr Betriebssystem und Ihre Browser-Software sollten stets dem aktuellen Versionsstand entsprechen.

Wie Sie Trojaner erkennen

Da sich Trojaner in der Regel unbemerkt vom Nutzer auf dem Computer installieren, werden sie erst mit Hilfe eines Antiviren-Programms sichtbar, dass die schädliche Software löscht.

Im **VR-ComputerCheck** finden Sie eine Liste mit Links zu kostenlosen Downloads von Virenschutz-Programmen und Firewalls. Sie finden den VR-ComputerCheck im Internet-Auftritt Ihrer Bank unter Konto & Karten / Sicherheit.

VR-ComputerCheck

Sicherheits-Tipps

ComputerCheck starten

Der VR-ComputerCheck kann mehrere Sicherheitsanforderungen auf Ihrem Computer prüfen. Er hilft Ihnen, die gefundenen Fehler zu beheben, damit wir Ihnen vom Zugriff auf die Online-Banking-Angebote der teilnehmenden Sparkassenbanken gesichert ist.

PC-Kenntnisse prüfen

Die Prüfpunkte

Informationen

Aktuelle Meldungen

Startknopf

Drücken Sie den Startknopf, um Ihren persönlichen VR-ComputerCheck zu starten.

Basisprüfung (1 min)

Auf den folgenden Seiten finden Sie weitere ausführliche und verständliche Hinweise für die Sicherheit Ihres Computers und Ihres Online-Bankings. Lesen Sie die Hinweise aufmerksam.

Wenn Sie Fragen haben, wenden Sie sich an den Berater in Ihrer Filiale. Er gibt Ihnen gerne Auskunft.



Diese Hinweise sollten Sie beachten

PIN und TAN gehen nur Sie was an

- Speichern Sie vertrauliche Daten wie Ihre Persönliche Identifikations-Nummer (PIN), Transaktions-Nummern (TAN) oder andere Passwörter nicht auf Ihrer Festplatte.
- Ändern Sie regelmäßig Ihre PIN.
- Geben Sie nie per E-Mail persönliche Daten wie Bankkonten, PIN und TAN, Kreditkarten-Daten oder Passwörter preis.
- Lassen Sie den Online-Zugang sofort sperren, falls Sie Ihre TAN-Liste verlieren.
- Vergewissern Sie sich, ob die auf der Internet-Seite geforderten Eingaben in Zusammenhang mit der von Ihnen gewünschten Aktion sinnvoll sind.
- Aktivieren Sie Ihre Spam-Filter. Alle großen Provider haben typische Phishing-Absender in ihre Filter aufgenommen.

Sicherheit der Internet-Verbindung

- Benutzen Sie für das Online-Banking keine Rechner in Internet-Cafés; hier sind Manipulationen Tür und Tor geöffnet.
- Halten Sie Ihr Betriebssystem sowie Browser-, Antiviren- und Firewall-Software aktuell. Im **VR-ComputerCheck** (im Internet-Auftritt Ihrer Bank unter Konto & Karten / Sicherheit) finden Sie eine Liste mit Links zu kostenlosen Downloads von Virenschutz-Programmen und Firewalls.
- Wenn Sie über ein Funknetz (WLAN) ins Internet gehen: Achten Sie darauf, dass die Daten-Übertragung ausreichend verschlüsselt ist.
- Auch Eingaben in Funktastaturen sind nicht abhörsicher. Verzichteten Sie deshalb in Büros und Mehrfamilienhäusern möglichst auf solche Tastaturen.
- Installieren Sie nur Programme auf Ihren PC, deren Herkunft Sie als vertrauenswürdig und seriös einschätzen.
- Löschen Sie alle E-Mails, deren Herkunft Sie nicht kennen.
- Klicken Sie keine Links oder Datei-Anhänge in E-Mails an, deren Herkunft Sie nicht kennen.
- Schließen Sie stets alle anderen Browser-Fenster, bevor Sie die Online-Banking-Anwendung starten.
- Deaktivieren Sie die Zusatzfunktion „ActiveX“ in Ihrem Browser (beim Internet Explorer unter Extras/Internetoptionen/Sicherheit => „Stufe anpassen“).
- Surfen Sie nicht mit Administrator-Rechten im Internet. Denn dann haben auch Angreifer aus dem Internet Administrator-Rechte auf Ihrem Computer. Legen Sie deshalb in der System-Steuerung von Windows unter „Benutzerkonten“ einen neuen Benutzer mit dem Kontotyp „Eingeschränkt“ an. Mit diesem surfen Sie im Internet (gilt ab Windows 2000).
- Geben Sie persönliche Daten grundsätzlich nur über SSL-verschlüsselte Internet-Seiten weiter und auch nur an Unternehmen, denen Sie vertrauen. Online-Banking ist eine solche SSL-gesicherte Anwendung. Sie erkennen eine



verschlüsselte Verbindung daran, dass die URL mit "https://" beginnt.

- Prüfen Sie, ob die in der Adresszeile des Browsers angegebene Internet-Adresse mit der zertifizierten Adresse Ihrer Bank übereinstimmt. Die zertifizierte Adresse erhalten Sie per Doppelklick auf das Schloss-Symbol unten rechts im Browser (beim Internet-Explorer bis Version 6).
- Klicken Sie nicht auf Links in E-Mails, Internet-Seiten oder sonstigen Nachrichten, um auf Ihre Bankseite zu kommen!
- Geben Sie die Adresse Ihrer Bank von Hand in die Adresszeile Ihres Browsers.
- Überprüfen Sie stets die Adresszeile Ihrer Online-Banking-Anwendung. Selbst durch kleine Änderungen könnten die Daten, die Sie eingeben, auf eine gefälschte Internet-Seite gelangen.
- Schließen Sie die Banking-Anwendung immer über die Logout- oder Abmelde-Funktion.
- Löschen Sie den Zwischenspeicher (Cache) nach jedem Besuch der Banking-Anwendung.
- Wenn Sie den Verdacht haben, dass die vorliegende Seite manipuliert ist, verlassen Sie diese und befolgen Sie keinesfalls die dort angegebenen Anweisungen. Informieren Sie Ihren Bankberater über die auffällige Seite.

Im Verdachtsfall

- Löschen Sie Phishing-Mails sofort, auch aus dem Papierkorb Ihres Computers oder Mail-Programms.
- Ignorieren Sie Links, die in Phishing-Mails hinterlegt sind. Hier könnte sich ein schädliches Computer-Programm verbergen.
- Sichern Sie regelmäßig Ihre selbst erstellten Dateien auf externen Speichermedien (zum Beispiel auf CD-ROM oder DVD). Falls ein Virus Ihr System beschädigt, können Sie auf diese Kopien zurückgreifen.
- Überprüfen Sie regelmäßig alle Buchungen auf Ihrem Konto; teilen Sie Unstimmigkeiten sofort Ihrem Bankberater mit.
- Informieren Sie sofort Ihre Bank, wenn Sie Daten in gefälschte Internet-Seiten eingegeben haben oder wenn Sie einen anderen Verdachtsfall haben. Zum Beispiel wenn die Verbindung während der Online-Banking-Anwendung abbricht. Sie können Ihr Konto sperren, indem Sie drei ungültige TAN eingeben.
- Lassen Sie im Schadensfall sofort die Überweisung zurückrufen, und erstatten Sie Anzeige.

So wählen Sie eine sichere Geheimzahl

Die Persönliche Identifikations-Nummer (PIN) ist – wie der Name schon sagt – eng mit Ihrer Person verbunden. Gerade beim Online-Banking ist es wichtig, dass die PIN außer Ihnen niemandem in die Hände fällt. Auch nicht mit Hilfe elektronischer Wörterbücher oder Suchmaschinen.

Was Sie vermeiden sollten

- Vermeiden Sie leicht zu erratende Kennwörter wie gleiche Zeichen und bekannte Zeichenfolgen (12345, 4711 oder 0815) oder Geburtstage, Postleitzahlen, Telefon-Nummern.
- Verwenden Sie auch keine Wohnorte oder Namen von Haustieren oder Familien-Angehörigen als PIN, auch keine Kombinationen wie „Tim32“ oder „1Moni9“.
- Computer-Hacker können einfache Tastenfolgen wie „qwertz“, „12345“ leicht knacken, auch wenn Sie Buchstaben und Ziffern kombinieren: „abcd09“.
- Vermeiden Sie gebräuchliche Abkürzungen wie „ISDN“, „GmbH“ oder „NRW“, um mit deren Hilfe eine PIN zu bilden.
- Speichern Sie PIN und TAN weder auf Ihrer Festplatte noch auf Zettel oder Schreibtisch-Unterlagen in der Nähe Ihres Computers.

Merkmale einer sicheren PIN

- Stellen Sie Ihre PIN aus Buchstaben und Zahlen zusammen.
- Verwenden Sie generell für unterschiedliche Zugänge (E-Mail, Online-Banking, Arbeitsplatz) möglichst unterschiedliche Passwörter.
- Eine sichere PIN erhalten Sie, wenn Sie zum Beispiel einen Satz als Eselsbrücke verwenden, den Sie sich gut merken können. Zusätzlich können Sie „i“ durch „1“ austauschen oder umgekehrt. So wird aus „Klaus ist ein versierter Heimwerker“ die PIN „k1evh“.
- Ändern Sie Ihre PIN regelmäßig.

Weitere Informationen im Internet

Wissenswertes zum Thema Internet-Sicherheit finden Sie – einfach und verständlich erklärt – auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

>> www.bsi-fuer-buerger.de

Kontogegenblatt für das Girokonto ...

für die Zeit

vom

bis zum

Schule:

Übertrag vom
Vormonat dem ...

Beleg Lfd. Nr.	Tag (Buchungs- datum)	Einzahler/ Empfänger	Zahlungsgrund/ Verwendungszweck	Einnahmen (Betrag in Euro)	Ausgaben (Betrag in Euro)	Bestand (Betrag in Euro)	Kontoauszug ausgedruckt am: (Datum)	erledigt durch: (Name des/der Ausführenden)
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								

Beleg Lfd. Nr.	Tag (Buchungs- datum)	Einzahler/ Empfänger	Zahlungsgrund/ Verwendungszweck	Einnahmen (Betrag in Euro)	Ausgaben (Betrag in Euro)	Bestand (Betrag in Euro)	Kontoauszug ausgedruckt am: (Datum)	erledigt durch: (Name des/der Ausführenden)
32								
33								
34								
35								
36								
37								
38								
39								
40								
41								
42								

Sachlich und rechnerisch richtig:

Übertrag für den
nächsten Monat

Unterschrift Schulleiter/in

