Zeitung in der Schule

Zisch

MIT FREUNDLICHER UNTERSTÜTZUNG VON:
Kreissparkasse Ludwigsburg

26

WWW.LKZ.DE

Diese Seite wurde gestaltet von der 8b der Realschule am Aurain Bietigheim-Bissingen

Stimmen

Was hat dir am Projekt besonders gefallen?

„Es war interessant und eine schöne Erfahrung, auch einmal eine Bank von innen zu sehen. Wir haben dort viel über Online-Banking gelernt."
Josia

„Ich finde gut, dass man Online-Banking auch schon in unserem Alter nutzen kann, wenn man sich an die Sicherheitsvorkehrungen hält."
Allison

„Bei dem Projekt haben wir viel über Online-Banking gelernt. Am interessantesten fand ich, dass man es auch schon als Jugendliche/r nutzen kann."
Mia

„Ich finde es gut, dass wir die Gefahren und Probleme von Online-Banking kennengelernt haben. Der Besuch in der Kreissparkasse war sehr interessant."
Nelson

Fallbeispiel Enkeltrick

Wie der Betrugsversuch per Whatsapp abläuft

Frau Müller, 74 Jahre alt, erhält eine Whatsapp-Nachricht von einer unbekannten Nummer: „Hallo Mama, mein Handy ist kaputt, das ist meine neue Nummer. Ich bin gerade in einer Notlage und brauche dringend Geld. Ich hatte einen Autounfall und muss sofort 3.500 Euro für die Reparatur überweisen. Bitte hilf mir, ich kann gerade nicht telefonieren." Frau Müller denkt, es handelt sich um ihre Tochter. In Sorge überweist sie den geforderten Betrag auf das angegebene Konto – erst später wird klar, dass es sich um Betrug handelte. Die echte Tochter wusste von nichts. Was lernen wir daraus? Betrüger geben sich geschickt als Familienangehörige aus – oft mit emotionalen Geschichten und Zeitdruck. Besonders ältere Menschen werden gezielt angesprochen.

Wichtig: Rufen Sie die betreffende Person unter der bekannten Nummer zurück – niemals auf die neue Nummer reagieren, ohne es zu prüfen. Überweisen Sie niemals Geld, ohne sicherzugehen, wer dahintersteckt. Im Zweifel: Polizei verständigen oder Bank kontaktieren.

VON LAURA, EMMA, EVA, LILOU, ANTON UND ANNA

ZEITUNG IN DER SCHULE

Informationen rund um das Zisch-Projekt

Im Projekt Zisch – Zeitung in der Schule lernen Schüler die Leseformate digital und gedruckt kennen, gewinnen einen Überblick darüber, was Zeitung beinhaltet, wie sie aufgebaut ist und wie Nachrichten recherchiert werden. Die Schüler werden selbst zu Journalisten, indem sie im Klassenverbund eine Zeitungsseite für die LKZ/den NEB gestalten. Jährlich nehmen circa 1.400 Schüler teil.

■ **Für Schulen und Lehrer:** Wenn Sie am Zisch-Projekt teilnehmen möchten, wenden Sie sich bitte an Markus Moog vom IZOP-Institut, Tel. (0 24 08) 58 89 19 oder per Mail an mm@izop.de. (red)

Die Klasse 8b vor der Kreissparkasse Ludwigsburg vor dem riesigen Sparschwein Louise. Foto: privat

Thema

Wie man sich online schützt

Die Klasse lernt, welche Gefahren bei finanziellen Transaktionen über das Internet bestehen

LUDWIGSBURG

Online-Banking gehört für viele Menschen längst zum Alltag. Es bezeichnet die Abwicklung von Bankgeschäften über das Internet. Dazu zählen zum Beispiel das Prüfen des Kontostands, das Tätigen von Überweisungen, das Einrichten von Daueraufträgen oder das Abrufen von Kontoauszügen – und das jederzeit, bequem von zu Hause oder unterwegs über den Computer, das Tablet oder das Smartphone. Doch wo Geld im Spiel ist, sind Betrüger nicht weit. Gerade im digitalen Raum lauern zahlreiche Gefahren. Wir, die Klasse 8b der Realschule im Aurain in Bietigheim-Bissingen, besuchten im April die Kreissparkasse in Ludwigsburg.

Bei einem interessanten Vortrag von Herr Nickel, einem Mitarbeiter der Kreissparkasse Ludwigsburg, erfuhren wir alles über Online-Banking, seine Gefahren, die Sicherheitsvorkehrungen der Kreissparkasse. Vor allem, wie man sich als Nutzer wirksam schützen kann. Besonders spannend war es, zu erfahren, dass auch wir als Jugendliche bereits Online-Banking nutzen dürfen. Umso wichtiger ist also die Aufklärung, damit dabei nichts schief geht.

Um Online-Banking sicher zu machen, gibt es von der Kreissparkasse folgende Sicherheitsvorkehrungen:

■ **Eine persönliche Identifikationsnummer (PIN):** Das ist so etwas wie ein geheimer Schlüssel, mit dem man sich bei seiner Bank einloggst. Man braucht ihn, um auf sein Konto zuzugreifen. Die PIN sollte man niemandem verraten und auch nicht im Handy oder auf dem Computer speichern.

■ **Eine Transaktionsnummer (TAN):** Das ist ein einmaliges Passwort, das braucht man, wenn man zum Beispiel eine Überweisung macht. Jede TAN ist nur für eine bestimmte Aktion gültig – damit wird verhindert, dass jemand anderes einfach Geld vom Konto überweist.

■ **Eine PushTAN:** Hier bekommt man die TAN direkt auf das Smartphone oder Tablet geschickt – über eine spezielle App der Bank. Man braucht also kein extra Gerät. Diese Methode ist sicher, solange man sein Handy gut schützt (zum Beispiel mit PIN, Fingerabdruck oder Gesichtserkennung).

■ **Eine ChipTAN:** Bei diesem Verfahren benutzt man ein kleines Gerät (den TAN-Generator) und die Bankkarte. Damit erzeugt man selbst eine TAN – zum Beispiel, indem man einen Code vom Bildschirm der Bank-Website einscannt. Das ist besonders sicher, weil nichts über das Internet übertragen wird.

Die häufigsten Tricks von Betrügern

Betrüger werden jedoch immer einfallsreicher. Zu den häufigsten Maschen gehören:

• Enkeltrick per Nachricht: Eine SMS oder WhatsApp-Nachricht gibt sich als Familienmitglied aus, das dringend Geld benötigt – etwa wegen eines Unfalls.

• Messenger-Betrug: Nachrichten wie „Hallo Mama, das ist meine neue Nummer" zielen darauf ab, Vertrauen zu erschleichen.

• Phishing-Mails: E-Mails im Namen von Banken fordern dazu auf, einem Link zu folgen oder Daten einzugeben. Diese Nachrichten sind gefälscht.

• Anrufe angeblicher IT-Mitarbeiter: Betrüger geben sich beispielsweise als Microsoft-Support aus, installieren Trojaner und spionieren den Computer aus.

• Social Engineering: Hierbei versuchen Kriminelle, Betroffene zu manipulieren – etwa durch fingierte Bankanfragen zur TAN-Freigabe.

Ein starkes Passwort ist die erste Schutzmauer. Es sollte mindestens 14 bis 16 Zeichen lang sein und aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen bestehen. Namen, Geburtsdaten oder Wörter aus dem Wörterbuch sollten vermieden werden. Gleiches gilt für die PIN. Diese sollte nicht digital aufbewahrt werden – persönliche Informationen wie Geburtsdaten oder einfache Zahlenfolgen sind als PIN ungeeignet.

Die Grundregel: Folgen Sie keinen Links aus E-Mails oder Nachrichten, bei denen Sie nicht sicher sind, wer der Absender ist. Ihre Bank wird Sie nie per E-Mail oder Anruf nach sensiblen Daten fragen.

VON CÖMERT, ALEX, ANDREAS, JONAS, NELSON, GIULIANO, DENNI, JOSIA, ELISA, ANTON S., CHRISTOS

Mehr Sicherheit fürs Konto

Diese Tipps bewahren vor digitalen Betrugsmaschen bei Online-Banking

Mit diesen einfachen Maßnahmen schützen Sie Ihr Konto zuverlässig vor Betrug und unbefugtem Zugriff:

■ **Immer abmelden:** Nach jeder Sitzung sollten Sie sich konsequent aus Ihrem Online-Banking abmelden – besonders auf gemeinsam genutzten Geräten.

■ **Benachrichtigungen aktivieren:** Viele Banking-Apps bieten Sicherheitsmeldungen an. So erfahren Sie sofort, wenn sich jemand in Ihr Konto einloggt.

■ **Kontobewegungen im Blick behalten:** Prüfen Sie regelmäßig Ihren Kontostand und achten Sie auf unbekannte oder verdächtige Abbuchungen.

■ **Sichere TAN-Verfahren nutzen:** PushTAN oder ChipTAN bieten zusätzlichen Schutz bei Überweisungen – besser als einfache SMS-TANs.

■ **Systeme aktuell halten:** Installieren Sie Updates für Ihr Smartphone, Ihren Computer und Ihre Banking-App immer sofort – Sicherheitslücken werden so geschlossen.

■ **Zwei-Faktor-Authentifizierung einrichten:** Wenn Ihre Bank es anbietet, aktivieren Sie diese Funktion. Sie bietet eine zusätzliche Sicherheitsebene beim Login.

Im Notfall sollte schnell gehandelt werden. Wenn Sie vermuten, dass jemand unbefugt auf Ihr Konto zugreift oder Sie Opfer einer Betrugsmasche geworden sind, heißt es: sofort reagieren! Rufen Sie den Sperr-Notruf 116 116 (kostenfrei) an – hier können Sie Ihre Bankkarte, Ihr Online-Banking oder auch Ihr Handy umgehend sperren lassen.

VON JULE, MIA, JOSI, GIULI, ALLISON, ESTEFANIA, ALENA UND ZOE