

# Online-Gangstern nicht ins Netz gehen

Safer Internet Day: Kriminalhauptkommissar Michael Rühl und Rechtsanwältin Melina Eberts von der Verbraucherzentrale über Betrugsmaschen und Datendiebstahl



MICHAEL RÜHL VOM POLIZEIPRÄSIDIUM SÜDHESSEN WEISS, WIE HACKER IM INTERNET DATEN KLAUEN. ER IST ZUSTÄNDIG FÜR DIE FACHBERATUNG CYBERCRIME. BILD: BERNO NIX

Von Petra Schäfer

**Biblis.** Die Vielfalt an digitalen Angeboten ist groß. Mit Verwandten und Freunden chatten oder sich im Internet Kleidung, Lebensmittel oder Medikamente bestellen, alles ist nur mit wenigen Klicks auf dem Mobiltelefon, Laptop oder PC möglich. „Gerade für ältere Menschen, die in ihrer Mobilität eingeschränkt sind, bringt das viele Vorteile“, stellte der Hauptamtliche Kreisbeigeordnete Matthias Schimpf bei einer Veranstaltung zum Aktionstag Safer Internet Day im Bibliser Rathaus fest.

Das Präventionsteam des Kreises Bergstraße sprach mit den Vorträgen der Experten besonders Seniorinnen und Senioren an. Das Motto hieß: „Online-Gangstern nicht ins Netz gehen.“ Was Kriminalhauptkommissar Michael Rühl vom Polizeipräsidium Südhessen und Melina Eberts von der Verbraucherzentrale Hessen über Betrugsmaschen und Schockanrufe zu sagen hatten, war allerdings für Zuhörer jedes Alters interessant.

### **Internet mit Bedacht nutzen**

„Es ist wichtig, das Internet mit Bedacht zu nutzen. Risiken müssen erkannt werden“, sagte Matthias Schimpf. „Daten können abgerufen und missbraucht werden. Der Schaden dadurch ist immens.“ Deshalb sei Aufklärung und Prävention so wichtig, betonte der Bibliser Bürgermeister Volker Scheib. „Das ist ein gesellschaftliches Thema, man muss sich damit beschäftigen.“

Michael Rühl von der Fachberatung Cybercrime beim Polizeipräsidium Südhessen zählte eine Reihe von Schadsoftware auf, die darauf aus ist, Daten zu sammeln oder auch Dateien auf dem Handy oder PC zu verändern und zu blockieren. Er rät daher, regelmäßig Dateien auf externen Festplatten zu speichern. Auch ein Virenschutzprogramm und sichere Passwörter sollten verwendet werden. Entscheidend sei jedoch auch das eigene Klick-Verhalten bei unbekanntem Anhängen. „Bei ungewöhnlichen E-Mails nicht sofort klicken, sondern darüber nachdenken. Wenn ich gerade bei Amazon bestellt habe und dann die Bestätigung per E-Mail kommt, ist das nachvollziehbar. Aber wenn ich so eine E-Mail erhalte und nichts bestellt habe, ist das verdächtig.“ Deshalb sollten in einer solchen Mitteilung keine Links angeklickt und auch keine persönlichen Angaben gemacht werden. Am besten löschen und sich direkt an das Unternehmen wenden oder auf dem gewohnten Weg das eigene Kundenkonto anschauen.

Dass die eigene Hausbank von ihren Kunden per E-Mail persönliche Daten und Passwörter einfordert, sei ausgeschlossen. „Cyber-Kriminelle arbeiten mit Zeitdruck. Lassen Sie sich nicht unter Druck setzen. Rufen Sie in so einem Fall bei Ihrem Geldinstitut an und fragen Sie nach.“

Den persönlichen Kontakt empfiehlt der Kriminalhauptkommissar auch bei außergewöhnlichen Mitteilungen, die angeblich aus dem Familien-, Freundes- und Bekanntenkreis kommen und bei denen es um Geldforderungen geht. „Es kann sein, dass E-Mail-Programme gehackt werden.“ Dann kommen die Mails nicht von den Freunden, sondern von Hackern. Also auch bei solchen Fällen hilft ein Anruf und eine persönliche Nachfrage.

Um Geld geht es auch bei den sogenannten Schockanrufen. Und dazu ist kein modernes Mobiltelefon nötig, die erreichen auch simple Schnurtelefone, wie eine Besucherin bei der Veranstaltung berichtete. Die Angerufenen werden in den Gesprächen enorm unter Druck gesetzt, indem Horrorgeschichten erzählt werden. Wie zum Beispiel, dass ein Familienangehöriger einen Unfall mit Personenschaden verursacht hat und in Haft ist. Schließlich wird eine Geldsumme gefordert, um ihm zu helfen.

Oder falsche Polizisten melden sich und wollen bei den Angerufenen wertvolle Gegenstände abholen, um sie angeblich vor Einbrechern zu schützen. „Lassen Sie sich auf keine Diskussionen ein. Legen Sie sofort auf und rufen Sie die Polizei an.“ Am besten sei es, sich Telefonnummern von Polizei und vertrauten Personen auf einem Zettel zu notieren, der immer griffbereit neben dem Telefon liegt und besonders in stressigen Situationen hilft, Familie und Freunde schnell zu erreichen.

Bei Herzensangelegenheiten im Internet rät Michael Rühl ebenfalls dazu, vorsichtig zu sein. Dort suchen digitale Heiratsschwindler Kontakt zu einsamen Seelen. Und nach einem netten E-Mail-Austausch wird plötzlich nach Geld gefragt, um zum Beispiel die Fahrt zu einem persönlichen Treffen bezahlen zu können. Erst seien es kleine Beträge und dann größere Summen. „Schauen Sie sich bei der Partnersuche vor Ort um, gehen Sie in Vereine. Lernen Sie sich persönlich kennen.“

### **Bewertungen lesen**

Vor Fakeshops im Internet warnte Rechtsanwältin Melina Eberts. Warnzeichen seien auffallend günstige Preise, die es sonst nirgends gebe.

Wichtig sei es, auf eine sichere HTTPS-Verbindung zu dem Online-Shop zu achten. Vorsicht sei bei Zertifikaten angesagt, mit denen Händler um Vertrauen werben. Diese können leicht selbst entworfen werden. Handelt es sich um ein anerkanntes Gütesiegel wie Trusted Shops müsse darauf geachtet werden, dass es aktuell ist.

„Lesen Sie Bewertungen, bevor Sie bestellen und nicht erst, wenn es Probleme gibt“, sagt Eberts. Wenn sich Leute beschwerten, dass die bestellte Ware nicht ankomme, sollte das beachtet werden. Die Rechtsanwältin rät zu sicheren Bezahlmethoden wie Kauf auf Rechnung oder aber Visa und Mastercard, bei denen eine sofortige Zurückerstattung des gezahlten Geldes möglich sei. Wer bereits Ärger mit Interneteinkäufen habe, könne sich Rat bei der Verbraucherzentrale holen. Eine Beratung koste rund 20 Euro.

---