|  |
| --- |
| **Musterbrief: Schutz vor Nicknapping** |
| Liebe Kolleginnen und Kollegen,  aktuell mussten wir feststellen, dass Schüler das Internetprofil einer Kollegin benutzt und Einkäufe im Internet getätigt haben. Dieser Identitätsmissbrauch kann schwere Folgen haben. Zur Vorbeugung vergleichbarer Fälle empfiehlt die Schulleitung Folgendes:  **1. Besuchen Sie nur sichere Websites**  Bevor Sie sensible persönliche Daten eingeben, sollten Sie sich sicher sein, dass die Website auch tatsächlich den neuesten Sicherheitsstandards entspricht. Erkennen können Sie dies an den Buchstaben „https“ in der Adresszeile Ihres Browsers und an einem Schloss- oder Schlüsselsymbol.  **2. Verwenden Sie sichere Kennwörter**  Verzichten Sie darauf, Ihren Vor- und Zunamen, Ihr Geburtsdatum oder den Namen Ihres Hundes als Passwort zu verwenden. Vielmehr sollten Sie eine Kombination von Buchstaben und Sonderzeichen verwenden. Ein sicheres Passwort können Sie unter https://www.passwort-generator.com erstellen lassen.  **3. Vorsicht bei unbekannten E-Mails!**  Nicht selten bekommen Sie E-Mails von Personen, die Sie nicht kennen, oder von Absendern, die Ihnen bekannte Personennamen verwenden. Checken Sie zunächst, wer hinter dem Absender steckt. Hierzu genügt es, dass Sie mit der Maus auf den Namen gehen, ohne diesen anzuklicken. Neben dem Namen erscheint die E-Mail-Adresse. Wenn diese Ihnen unbekannte Namen oder Zeichen enthält oder eine ausländische Kennung trägt, wie z. B. „.ru“ für Russland, sollten Sie aufpassen. Öffnen Sie die E-Mail nicht.  **4. Vermeiden Sie ungeschützte WLAN-Zugänge**  WLAN-Zugänge an öffentlichen Plätzen agieren unverschlüsselt. Damit tragen Sie ein hohes Sicherheitsrisiko, wenn Sie über solche offenen WLAN-Systeme auf Ihre persönlichen Daten zugreifen z. B. auf Ihr Online-Banking.  Für Rückfragen steht Ihnen gern auch unser schuleigener Datenschutzbeauftragter, der Kollege *Jan Becker*, zur Verfügung.  Mit freundlichen Grüßen  *Christoph Weber*  Schulleiter |