AZ 3780 Gstaad 145. Jahrgang Nr. 36 **Freitag, 9. Mai 2025**

Anzeiger von Saanen

HEUTE GROSSAUFLAGE

www.anzeigervonsaanen.ch Einzelverkaufspreis Fr. 2.10

Die Zeitung für die Gemeinden Saanen, Gsteig und Lauenen

Hart verdientes Geld wird leicht gestohlen

Im digitalen Universum ist es einfach, falsche Identitäten zu bauen und damit andere in die Irre zu führen: falsche Enkel, gefakte Liebe, getürkte Angebote und nicht existierende Geldanlagen.

SYMBOLBILD: PEXELS

Die vor Kurzem erschienene polizeiliche Kriminalstatistik 2024 zeigt: Die Straftaten, die der digitalen Kriminalität zugeordnet werden, haben im vergangenen Jahr um 43 Prozent zugenommen. Die Cyber-Wirtschaftskriminalität bildet dabei mit 7705 (das sind bei 365 Tagen rund 21 Delikte pro Tag, also fast eine pro Stunde rund um die Uhr) registrierten Straftaten und einer Zunahme von 45 Prozent den mit Abstand grössten Bereich.

Obschon sich die jeweiligen Betrugsmuster stark ähneln, gelingt es betrügerischen Gruppierungen immer häufiger, arglose Menschen hinters Licht zu führen. Auch im Saanenland wird die Polizei tagtäglich mit Cybercrime konfrontiert.

Adriano Di Camillo, Stv. Vorsitzender der Geschäftsleitung der Saanen Bank, Marc Schmid, CEO Schmid Gstaad AG, Anita Mani, Wachtchefin der Polizei Gstaad und Martin Bader, Spezialist Prävention Cybercrime bei der Kantonspolizei Bern, sprechen über ihre Erfahrungen.

Bericht: Seiten 10 und 11

Viele Opfer, doch kaum jemand spricht darüber

GESELLSCHAFT Die digitale Kriminalität hat im Vergleich zum Vorjahr um über 30 Prozent zugenommen. In vielen Fällen ist die Schwachstelle der Mensch, der zu vertrauensselig oder gutgläubig heikle Daten preisgibt und danach beraubt oder erpresst wird. Auch das Saanenland wird von Cyberattacken nicht verschont.

KEREM S. MAURER

Bei der genaueren Betrachtung einiger Fälle aus dem Saanenland mit Fachleuten von der Polizei sowie aus der Bank- und IT-Branche zeigt sich, dass das Opfer in vielen Fällen vielleicht zu arglos gehandelt hat, weil es Geld oder Daten gutgläubig und freiwillig an Dritte herausgegeben hat. Weil es auf eine betrügerische Masche hereingefallen ist. Anita Mani, Wachtchefin der Polizei in Gstaad, sagt: «Man muss die digitalisierte Kriminalität punkto Unfassbarkeit und Dimension als ein ganzes Universum betrachten, in dem gelogen wird, dass sich die Balken biegen.» Auf die Frage, wie oft die Polizei im Saanenland mit digitaler Kriminalität konfrontiert wird, sagt sie: «Es vergeht kaum ein Tag, am dem wir nicht in irgendeiner Form damit konfrontiert werden.»

> “
> Man muss die digitalisierte Kriminalität punkto Unfassbarkeit und Dimension als ein ganzes Universum betrachten, in dem gelogen wird, dass sich die Balken biegen.
>
> **Anita Mani**
> Wachtchefin Stationierte Polizei Gstaad

Die Betrugsmuster sind oft ähnlich

Martin Bader, Spezialist Prävention Cybercrime bei der Kantonspolizei Bern, sagt: «Viele Cyberbetrüge folgen einem ähnlichen Muster: Täter bauen unter falscher Identität Vertrauen auf, um ihre Opfer gezielt zu täuschen. In zahlreichen Fällen geht es letztlich darum, Menschen durch manipulatives Vorgehen zu betrügen.» Man solle sich, sein Umfeld und die Mitarbeitenden darüber informieren, wie emotionale Manipulation funktioniere. «Schutz vor Cyberkriminalität beginnt bei der Prävention», so Bader. Und Adrian Di Camillo, Stellvertretender Vorsitzender der Geschäftsleitung der Saanen Bank, gibt zu bedenken: «In der Regel ist Geld, das an Betrüger überwiesen wird, weg. Sobald es auf dem Konto der Betrüger eingeht, wird es weitergeleitet oder abgehoben.» Und er weist darauf hin, dass eine Bank nie via E-Mail oder Telefon die Preisgabe von Passwörtern oder Zugangsdaten fordere.

Firewalls, Sicherheits Updates und Passwortmanager helfen

«Oft liegen die Probleme nicht an der Technik, die ständig verbessert wird, sondern an der Schwachstelle Mensch», hält Marc Schmid, IT-Fachmann und Inhaber von Schmid Gstaad AG, fest. Er rät: «Wichtig ist, dass man die Systeme auf allen Geräten aktuell hält, regelmässige Sicherheitsupdates durchführt und Firewalls benutzt.» Es gebe auch technische Möglichkeiten, um schadenmindernd einzugreifen, nachdem eine Cyberattacke stattgefunden habe. «Nachdem ein Mitarbeiter ungeschickterweise eine schädliche Mail geöffnet hat und im Begriff ist, Daten an Dritte zu übermitteln, läuten technische Alarmglocken. Man kann schädliches Verhalten in einem Netzwerk erkennen und Schlimmstes verhindern», so Schmid. Die Zwei-Faktor-Authentifizierung, bei der angeforderte Zugangscodes auf ein zweites Gerät gesendet werden, bietet ebenfalls zusätzlichen Schutz. Wer so etwas einrichten möchte, findet Unterstützung in entsprechenden Geschäften. Zudem sei es ratsam, für jeden einzelnen Dienst ein anderes Passwort zu verwenden. Laut Schmid sind rund 80 Prozent jener, die in seinem Geschäft Hilfe betreffend digitaler Sicherheit suchen, ältere Leute, die nicht mit den ganzen digitalen Geräten aufgewachsen sind, aber: «Erschreckend hoch ist die Anzahl junger Menschen, die sich seit ihrer Kindheit im digitalen Universum bewegen und trotzdem oft sehr blauäugig agieren.»

> “
> In der Regel ist Geld, das an Betrüger überwiesen wird, weg. Sobald es auf dem Konto der Betrüger eingeht, wird es weitergeleitet oder abgehoben.
>
> **Adrian Di Camillo**
> Stv. Vorsitzender der Geschäftsleitung der Saanen Bank

Auch KMUs sind oft betroffen

«Leider tappen auch viele KMUs in die Falle», weiss Marc Schmid. Oft wisse man nicht, wie die Malware ins Netzwerk gekommen sei. Zielführend sei in einem solchen Fall eine korrekte Analyse durch den IT-Betreuer oder einen externen Gutachter. Wenn nicht sicher sei, ob alle Malware entfernt und allenfalls noch Schläfer vorhanden sind, sollten sämtliche Betriebs- und Schutzsysteme gepatcht, sprich aktualisiert werden. Auch Staubsaugerroboter, Smartlights, Kameras, Gegensprechanlagen TV-Geräte, Zutrittssysteme oder Drucker sollten im sogenannten Patch-Management enthalten sein. «Unternehmer:innen und Privatpersonen sollten sich einen Überblick verschaffen, was sie alles haben, um sich effektiv vor Cyberangriffen zu schützen», rät Schmid. Und es sei sinnvoll, in seinem Unternehmen jemanden zu motivieren, der sich über mögliche Verbesserungen im Cyberschutz sowie über aktuelle Cyberbedrohungen – die sich laufend verändern – informiert.

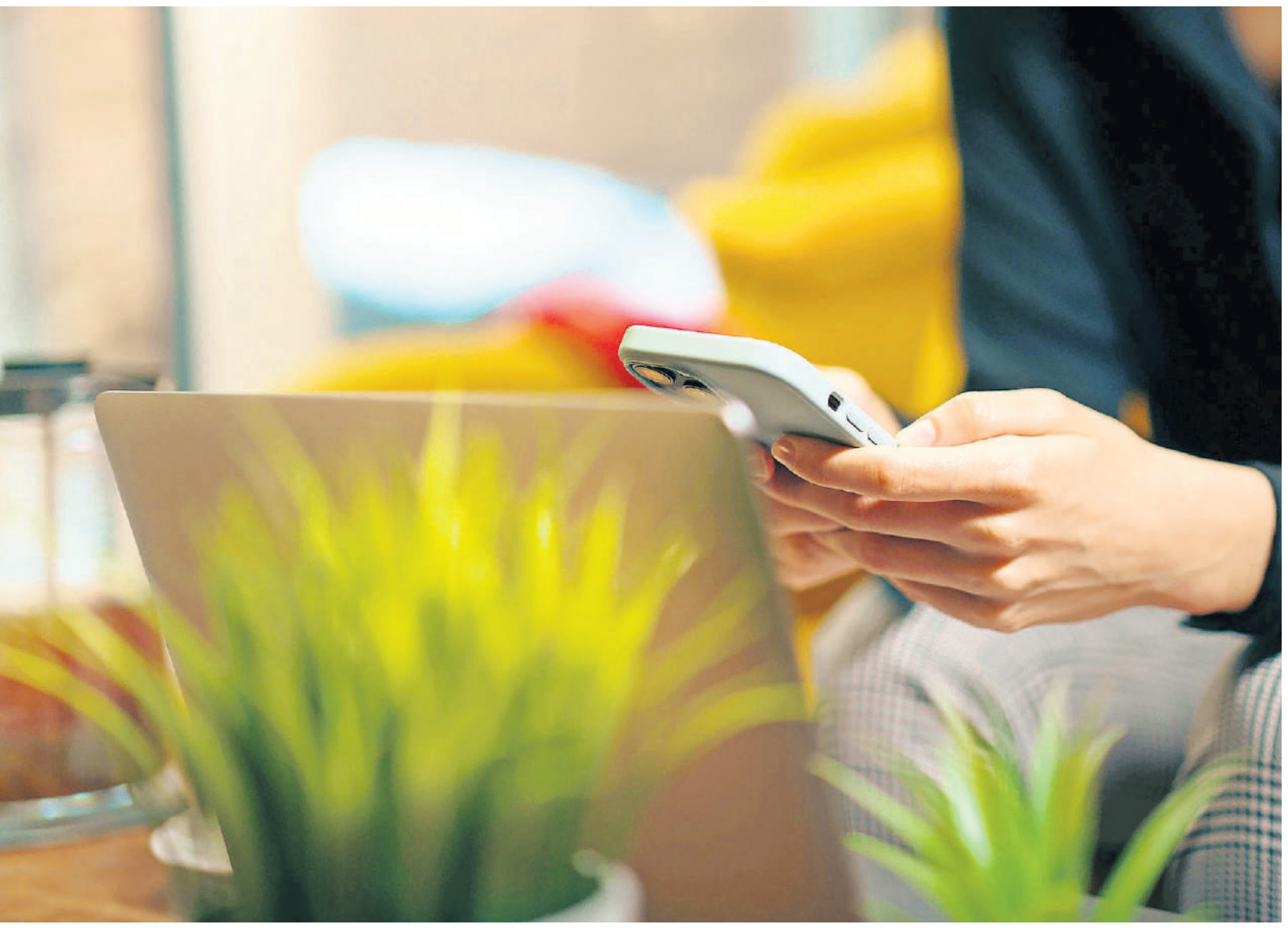
Verlockende Angebote überprüfen

Angebote, die zu gut sind, um wahr zu sein (Stichwort: Lockvogel), sind selten wahr, genauso wie jene, die zu krass erscheinen (Schockanruf). «Wir sollten uns öfter auf unser Bauchgefühl verlassen», sagt Anita Mani. Heisst konkret: Wenn einem etwas komisch vorkommt, lässt man besser die Finger davon. Und wenn man nicht sicher sei, ob das verlockende Angebot, das gerade auf dem Küchentisch liegt, echt ist oder nicht, könne man es mit jenen vergleichen, die auf cybercrimepolice.ch gelistet sind. «Auf dieser Website werden Phishing-Kampagnen und Betrugsmaschen aufgeführt, welche gerade im Umlauf sind», so Mani. Sinnvoll sei es auch, eine Telefonverbindung mit einem angeblichen Bankangestellten, Polizisten oder Netzbetreiber zu unterbrechen und beim entsprechenden Unternehmen direkt nachzufragen, ob man gerade von einem seiner Mitarbeiter angerufen worden sei. Und ganz wichtig: Keine persönlichen Daten, Bankdaten, Zugangsdaten, Passwörter, Kopien von Pass oder Identitätskarten oder Fotos und Filme, auf denen man leicht oder gar nicht bekleidet zu sehen ist und allenfalls sexuelle Handlungen vornimmt, irgendwohin senden. Insbesondere mit Letzterem werden viele Leute erpresst. Denn Fotos oder Filme, die einmal im Netz auftauchen, sind praktisch nicht mehr von dort zu entfernen.

Darüber reden hilft

Fazit: Im digitalen Universum sollte man den Kopf einschalten, gesunden Menschenverstand walten lassen und Dinge kritisch hinterfragen. Der enorme Druck, der durch Betrüger aufgebaut werde, sei normalerweise nicht real, sagt der Cybercrime-Präventionsspezialist der Berner Kantonspolizei. Es komme sehr selten vor, dass eine wildfremde Person anrufe und man daraufhin sofort handeln müsse. Und wenn man trotz aller Vorsicht doch einmal in eine Falle tappe, sei man damit nicht allein. «Es passiert sehr vielen Leuten – auch im Saanenland. Sprechen Sie darüber, erzählen Sie, was Ihnen passiert ist, damit anderen dasselbe nicht auch passiert», sagt Anita Mani.

Sie setzen sich von Berufs wegen täglich mit Fragen der Cybersicherheit auseinander und unterstützen ihre Kundinnen und Kunden bei Fragen. V.l.: Adriano Di Camillo, Stv. Vorsitzender der Geschäftsleitung der Saanen Bank, Rolf Schmid, Kundenberater und IT-Experte der Saanen Bank, Anita Mani, Wachtchefin der stationierten Polizei in Gstaad, und Marc Schmid, CEO Schmid Gstaad AG.
FOTO: KEREM MAURER



Es passiert sehr vielen Leuten, Opfer eines Cyberbetrugs zu werden. «Nicht schämen, besser darüber reden», empfiehlt Anita Mani von der Polizei. SYMBOLBILD: PEXELS

WAS TUN, WENN ICH AUF EINE BETRUGSMASCHE HEREINGEFALLEN BIN?

Wenn man sich trotz aller Vorsicht doch einmal von einem Angebot verlocken lässt und Geld oder Daten an Dritte weiterleitet, gilt folgendes Vorgehen:

- Bankkarten sofort sperren und Ihre Bank informieren. Ggf. eine neue Debitkarte beantragen.
- Wenn Sie die ID oder den Pass kopiert und an betrügerische Dritte übermittelt haben, lassen Sie die Dokumente bei der kantonalen Passstelle oder der Polizei annullieren.
- Anzeige erstatten. Entweder persönlich bei der Polizei oder via Meldeplattform https://www.suisse-epolice.ch
- Kartenlimite heruntersetzen.
- Sprechen Sie darüber und machen Sie die Masche bekannt.
- Machen Sie Screenshots des verdächtigen Angebots. Diese brauchen Sie für die Bekanntmachung und für allfällige Versicherungen.
- Ändern Sie sofort die Passwörter, die Sie weitergegeben haben.
- Warnen Sie Bekannte vor kriminellen Machenschaften, die in Ihrem Namen getätigt werden.
- Beim BACS unter https://www.report.ncsc.admin.ch/de/ melden. KMA

MELDEPFLICHT FÜR CYBERANGRIFFE AUF KRITISCHE INFRASTRUKTUREN GILT AB 1. APRIL

Laut einer Medienmitteilung der Schweizerischen Eidgenossenschaft hat der Bundesrat die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ab dem 1. April 2025 in Kraft gesetzt. «Die Betreiberinnen und Betreiber von kritischen Infrastrukturen werden verpflichtet, dem Bundesamt für Cybersicherheit (BACS) Cyberangriffe 24 Stunden nach deren Entdeckung zu melden», schreibt der Bund. Diese Meldungen sollen es dem BACS ermöglichen, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und Betreiber:innen kritischer Infrastrukturen frühzeitig zu warnen.

Als kritische Infrastrukturen gelten gemäss Informationssicherheitsgesetz (Art. 74b ISG) bestimmte Kategorien von Behörden und Organisationen, wie beispielsweise Bundes-, Kantons- und Gemeindebehörden, Betreiberinnen und Betreiber der Energie- und Trinkwasserversorgung, Gesundheitseinrichtungen auf kantonalen Spitallisten, Finanzinstitute, konzessionierte Transportunternehmen, registrierte Anbieter von Fernmeldediensten sowie grössere Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen, zu denen auch Grossverteiler wie Migros, Coop oder Denner gehören. Für viele dieser Kategorien gelten spezifische Schwellenwerte, unterhalb derer kleinere Organisationen von der Meldepflicht ausgenommen sind. KMA

Was tun, wenn es passiert ist? Die Experten für Cyberkriminalität geben wertvolle Verhaltenshinweise. SYMBOLBILD: PIXABAY

Fallbeispiele aus dem Saanenland

Ein angeblicher Microsoft-Mitarbeiter ruft an und meldet ein Sicherheitsproblem auf dem Gerät des Angerufenen. Um dieses zu beheben sei die Installation eines Programmes sowie die Auslösung einer Zahlung via E-Banking erforderlich. Die installierte Software greift derweil die Daten ab, leitet sie dem angeblichen Microsoft-Mitarbeiter weiter, worauf sich dieser Geld vom Konto des Angerufenen abhebt.

Jemand ruft an, erzählt die Tochter oder der Sohn sei in einen schweren Autounfall verwickelt, liege schwer verletzt in einem ausländischen Spital und brauche umgehend 10'000 Franken.

Man wird per E-Mail, das auf den ersten Blick so aussieht, als stamme es von einer Bank, einer Versicherung oder einem Netzanbieter, aufgefordert, Passwörter und Zugangsdaten mitzuteilen oder zu ändern. Diese Daten werden später missbraucht, um das Opfer zu schädigen.

Ein Anrufer unterbreitet dem Angerufenen eine Investitionsmöglichkeit mit tollen Renditen und will ihn dazu bringen, in eine nicht vorhandene Geldanlage zu investieren.

Via Online-Plattformen wird Ware bestellt und vorausbezahlt, aber nie geliefert. Oft sagen die angeblichen Verkäufer auch, dass das Bestellgut nicht geliefert werden kann, sondern abgeholt werden muss – allerdings ausschliesslich gegen Vorkasse.

Angeblich sehr attraktive, meist junge Frauen, gaukeln Männern grosses sexuelles Verlangen vor und bringen sie dazu, Nacktfotos oder Videos mit sexuellen Inhalten zu versenden. Die arglosen Männer werden dann mit dem so erhaltenen Foto- und Bildmaterial von der organisierten Gruppierung, die dahintersteckt, erpresst.

Jemand bucht eine Ferienwohnung, bezahlt üblicherweise im Voraus und stellt bei Ferienantritt fest, dass es sich bei der Adresse nicht um ein Ferienhaus, sondern um ein normales bewohntes Haus handelt.

Person X gibt sich als Person Y aus, schreibt ein E-Mail an den Personalverantwortlichen der Firma, bei der Y arbeitet, und gibt an, dass der Lohn künftig auf ein anderes Konto ausbezahlt werden soll. Die getäuschte Personalfachperson leitet die Salärzahlung von Y auf das von X angegebene Konto um. Y wird um sein hart verdientes Geld gebracht.

Eine Dame meldet, sie habe ihrem Liebhaber, den sie im Internet kennengelernt und noch nie gesehen habe, einen grösseren Geldbetrag geschickt, weil er in Not gewesen sei oder sie in der Schweiz besuchen wollte. Der Mann ist weg, das Geld auch. Von Liebe keine Spur.