Cyber-Risiken im Privatleben: Wie man sich vor vier typischen Gefahren der digitalen Welt schützt

Wirtschaft Finanzen Versicherung © Pixabay

Seit der Corona-Pandemie findet ein größerer Teil unseres Lebens als früher in den eigenen vier Wänden statt – und damit verstärkt online: Einkaufen, Bankgeschäfte, Arbeiten, sogar Treffen mit Freunden und Verwandten. Das machen sich Cyber-Kriminelle zunutze. Die VGH Versicherungen informieren über vier Cyber-Risiken, auf die man im privaten Umfeld besonders Acht geben sollte, und zeigen Lösungen auf.

Rund 40 Prozent der Deutschen werden jährlich Opfer von Cyber-Kriminalität. Das geht aus einer repräsentativen Umfrage des Meinungsforschungs-Instituts YouGov für den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hervor. „Die Kriminellen tummeln sich dort, wo sie leichtes Spiel haben und viele potenzielle Opfer antreffen“, sagt Melanie Fenske, Expertin für Cyber-Risiken bei der VGH. Die Angriffsfläche hat sich gerade in Zeiten der Krise bei Privatpersonen extrem vergrößert. Vier zentrale Risiken und wie sich Bürgerinnen und Bürger schützen können:

1. Betrug beim Online-Shopping

Online-Shopping erhöht das Risiko, Opfer von Cyber-Kriminalität zu werden. Vor allem bei unsicheren Zahlungsmethoden lauern Gefahren: Insbesondere die Option Vorkasse ist bei unbekannten oder ominösen Händlern keine Zahlungsmöglichkeit, die man wählen sollte. Hier gibt es keine Garantie, größere Summen nach einer fehlgeschlagenen Kaufabwicklung erstattet zu bekommen, wie es bei bekannten Online-Zahlungsdienstleistern der Fall ist. Betrüger, die sich als vermeintlich seriöse Händler ausgeben, haben häufig Firmensitze in den entlegensten Gegenden der Erde, besitzen keine AGB oder bieten ihre Ware zu utopischen Preisen an. Auch auf Gütesiegel sollten Verbraucher achten. Diese bestätigen Sicherheitsvorkehrungen der Shops,

die Betrug weitestgehend ausschließen. Bekannte Siegel sind zum Beispiel „Trusted Shops“ und das „S@fer-Shopping“-Gütesiegel vom TÜV SÜD.

2. Identitätsdiebstahl

Identitätsdiebstahl bedeutet den Missbrauch personenbezogener Daten durch Dritte. Die Täter versuchen, im Namen ihrer Opfer Produkte zu bestellen, Zugang zu deren Online-Banking zu erlangen, sich auf Social-Media-Plattformen zu positionieren oder andere Straftaten zu begehen. Ganz oben stehen hier extremistische Äußerungen und die Belästigung Minderjähriger. Für ahnungslose Nutzer liegt die Gefahr – neben einer öffentlichen Rufschädigung – ganz klar hier: Sie haften für die Straftat. „Um sich vor solchen Cyber-Risiken zu schützen, ist ein sicheres und oft wechselndes Passwort das A und O“, sagt VGH-Expertin Melanie Fenske.

Weil auch so genannte Phishing-Mails eine immer beliebtere Methode der Kriminellen sind, an sensible Daten zu gelangen, gilt hier ebenfalls Vorsicht: Mails sollten nur dann geöffnet werden, wenn sie von vertrauten Personen oder Unternehmen kommen, mit denen man kürzlich in Kontakt stand.

3. Cyber-Kriminalität im Home Office

Auch das Arbeiten von zu Hause bietet eine breite Angriffsfläche. „Cyber-Kriminelle kennen die Schwachstellen genau und nutzen diese rücksichtslos aus“, warnt Melanie Fenske. Wenn sich Mitarbeitende beispielsweise von ihrem privaten Gerät ins Firmennetzwerk einwählen, sind die Sicherheitslücken meist größer, und Updates müssen oft in Eigenverantwortung installiert werden. Zudem tarnen Internet-Kriminelle viele Angriffe in oft professionell gestalteten Phishing-Mails, die der aktuellen Lebens- oder Arbeitssituation ihrer Opfer angepasst sind.

Besonders verbreitet ist die „Fake President“-Masche, auch „CEO-Fraud“ genannt. „Bei dieser Methode geben sich die Betrüger als Führungspersonen aus. Sie versuchen, Mitarbeitende durch Ausnutzen ihrer vermeintlichen Autorität dazu zu bewegen, sensible Daten herauszugeben oder Geld auf ihre Konten zu überweisen“, erklärt Fenske. „Seien Sie also auch im Home Office wachsam!“

4. Cyber-Mobbing

Cyber-Mobbing wird häufig nicht ernst genommen, weil es nicht im „realen“ Leben stattfindet. „Diese Annahme täuscht“, warnt die VGH-Expertin. „Cyber-Mobbing ist nicht zu unterschätzen.“ Im digitalen Raum sinkt online oft die Hemmung, Mitmenschen zu provozieren, zu beleidigen oder zu bedrohen. Allgemein gilt deshalb immer: Verhaltensregeln, die im analogen Miteinander gelten, sollten auch online eine Tugend sein.

Cyber-Mobbing kann für die Opfer weitreichende Folgen haben: Senkung des Selbstwertgefühls, soziale Isolation und im schlimmsten Fall Suizidgedanken. Zahlreiche Organisationen stehen den Betroffenen zur Seite. Beim Bundesministerium für Familie, Senioren, Frauen und Jugend sind Anlaufstellen und anonyme Hilfenummern gelistet, an die man sich wenden kann. Auch die VGH Versicherungen helfen gerne weiter.

„Um im Schadenfall nicht in Panik zu geraten und gezielt Maßnahmen ergreifen zu können, ist der Abschluss einer Cyber-Versicherung sinnvoll“, weiß Fenske. Neben dem Schutz vor finanziellen Verlusten bietet eine Cyber-Versicherung umfassende Serviceleistungen und stellt Expertenwissen zur Verfügung. „Deshalb ist es ratsam, den persönlichen Schutz vor Cyber-Risiken gemeinsam mit einem unserer Berater zu überprüfen“, empfiehlt die Expertin der VGH Versicherungen.