Die digitale Welt ist ein Eldorado für Betrüger

Wenn Werbung lügt

Ob irreführende Werbeanzeigen, gefälschte SMS mit Hilferufen der eigenen Kinder oder gefakte Werbevideos mit prominenten Gesichtern, die zu lukrativen Investments raten – speziell die digitale Welt ist ein Eldorado für Betrüger.

Halbieren Sie Ihre Heizkosten mit der schnellen, energieeffizienten Technologie von EquiWarm Pro. Es heizt jeden Raum in nur 10 Minuten auf!“ – ist Ihnen diese oder ähnliche Werbung auch schon auf *Facebook, Instagram* oder *YouTube* begegnet? *Watchlist Internet* und der Verein zur Aufklärung über Internetmissbrauch *mimikama* raten zur Vorsicht bei Werbeanzeigen, in denen Produkte angepriesen werden, die wenig kosten und viel leisten sollen.

EquiWarm Pro, ein in China hergestelltes Miniheizgerät, das man direkt an eine Steckdose ansteckt, soll eine „Wunderheizung“ sein. Es wird als „Tesla der Heizgeräte“ beworben. Wer rasch bestellt, bekommt 50 Prozent Rabatt und zahlt statt 99,98 „nur“ 49,99 Euro. Bei Amazon wird das Gerät zum Beispiel um 25 Euro angeboten, bei der chinesischen Verkaufsplattform Alibaba.com ist es um 6 US-Dollar zu haben.

Eines der Verkaufsargumente für das Gerät in der Werbung in den sozialen Medien in Österreich und Deutschland lautet, dass es von zwei Amerikanern, Becker und Schmidt, erfunden worden sein soll. Für dieselbe Werbung in der digitalen Welt in Spanien heißen die „Erfinder“ Sanchez und Garcia, in Dänemark werden sie Andersen und Nielsen genannt, in Polen Nowak und Kowalski. Bewertungen von Konsumenten auf Trustpilot zum EquiWarm-Pro-Heizgerät lauten zum Beispiel: „Vorsicht, brandgefährlich! Diese Geräte haben in Europa keine Zulassung, weil sie mindere Werkstoffe verbaut haben. ... Die Firmen ... nehmen damit Brandkatastrophen in Kauf ...“ „Dieses Produkt ist eines von vielen chinesischen Produkten, die über You-Tube mit monumentalen Vorteilen gegenüber der Konkurrenz ... angepriesen werden. Es wird gelogen, wer dahinter steht, was das Produkt kann und es wird billigend in Kauf genommen, dass im schlimmsten Fall jemand zu Schaden kommt, denn die Geräte sind nicht sicher!“

Die Bestell-Webseite für das Heizgerät weist kein Impressum, keine Mail-Adresse oder Telefonnummer auf, um zu reklamieren. Das gilt auch für andere Geräte, die unter dem Namen „EquiWarm“ angepriesen werden, etwa die Hightech-Überwachung Opti-Guard, Viper-Charge, das schnellste Ladegerät der Welt, das Antischnarchgerät Tranquil-Air, die Hightech-Smartwatch Pulse-Tech, das Reinigungsgerät Scrub-Ninja, Photo-Guard, die Ultraschallzahnbürste Sense-Pro oder Photo-Tek zur Sicherung von Fotos und Videos – alles um 50 Prozent „günstiger“ für „Schnellbesteller“.

Bewertungen auf *Trustpilot* zum angeblich schnellsten Ladegerät der Welt Viper-Charge lauten zum Beispiel: „Habe das Gerät für ca. 50 Euro gekauft und habe festgestellt, dass das natürlich ein Fake ist. Dieses Ladegerät hat höchstens einen Wert von 5 Euro incl. Versand ...“

Eine andere Bewertung lautet: „Kontaktmöglichkeit fehlt und wer ist der Lieferant? Werbung erfolgt auf Deutsch, nach der Bestellung alles nur noch auf Englisch. China Kernschrott.“ Laut einer anderen Bewertung „braucht das Ladegerät genauso lange wie jedes herkömmliche Ladegerät. Hier wird massiv betrogen. Es gibt keine Möglichkeit diesen Schrott zurück zurückzuschicken.“

FOTO: STOCK.ADOBE.COM

Ein Entgiftungspflaster soll die körperliche und psychische Gesundheit mit Hilfe eines natürlichen asiatischen Entgiftungspflasters steigern, heißt es auf der Seite nuubu.com. Der zeitlich begrenzte Rabatt von 70 Prozent soll zu einem raschen Kauf verlocken. Ähnlich wie bei den Angeboten von EquiWarm werden die Rabatte auf Dauer angeboten.

Watchlist Internet rät zu Vorsicht, denn „die litauische Firma hält rechtliche Vorgaben beim angeblichen ‚Wunderheilmittel Entgiftungspflaster' nicht ein. Erfahrungsberichten zufolge komme es immer wieder zu Problemen bei der Wahrnehmung des Rücktrittsrechts sowie bei der Kommunikation mit dem Unternehmen."

Laut der *Watchlist* steckt hinter dem scheinbaren Wunderheilmittel die Firma „UAB Ekomlita" aus Litauen. Die Produktpalette dieser Firma reicht von Messern über Sofaüberzüge bis hin zu portablen WLAN-Routern. Ob die gemachten Versprechungen auf den unterschiedlichen Seiten tatsächlich eingehalten werden, können wir nicht beurteilen. Das gilt auch für das Entgiftungspflaster, das auf nuubu.com verkauft wird", heißt es auf *Watchlist Internet*.

Watchlist Internet ist eine unabhängige Informationsplattform zum Thema Internetbetrug. „Wir informieren Privatpersonen und Unternehmen zu aktuellen Betrugsfallen im Internet und geben Tipps, um sich davor zu schützen", erklärt Thorsten Behrens, Projektleiter von *Watchlist Internet*. „Prävention und Awareness-Bildung rund um das Thema Internetbetrug sind unsere Aufgaben. Wenn jemand zum Beispiel im Internet einkaufen möchte, bei einem Online-Shop ein seltsames Gefühl hat und dann nach dem Shop googelt, findet er im Idealfall unsere Warnmeldung ganz oben in den Suchergebnissen." Mehr als 250.000 Aufrufe verzeichnet die Plattform monatlich.

Internetfallen. Etwa 1.000 Internetfallen werden monatlich gemeldet, alleine über das Online-Meldeformular der *Watchlist Internet*. „Dazu kommen noch Meldungen von der Internet-Ombudsstelle, unserem Partner und Meldungen, automatisiert durch unseren Fake-Shop-Detector", erklärt Behrens. „Wir schauen bei allen Meldungen, ob es sich um Betrug handelt. Betrügerische Webseiten veröffentlichen wir auf unseren Listen. Warnmeldungen schreiben wir, wenn uns eine Falle entweder auf einmal sehr oft gemeldet wird, oder wenn es sich um eine neue oder weiterentwickelte Betrugsmasche handelt."

Kriminelle könnten mit KI-generierten Stimmen von Kindern oder Enkeln der Angerufenen Druck erzeugen, um von ihnen Geld zu erpressen.

Foto: Stock.Adobe.com

Den Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamts fällt auf, dass Werbeanzeigen für alle möglichen Produkte in der digitalen Welt zunehmen. In *Facebook* werden oft Profile übernommen, die reaktiviert wurden. In weiterer Folge wird das Profil umbenannt und als Werbeplattform benutzt. Wer es anklickt, kommt meist extern auf eine Fake-Seite mit kurzer Lebensdauer, wo man bestellt. Besonders beliebt ist die Kombination mit Nachnahmeversand. Man bestellt in diesem Fall ein „teures" Gerät äußerst günstig – zum Beispiel ein Samsung-Handy statt 1.490 um 199 Euro und erhält per Nachnahme eine wertlose Billigkamera.

Am häufigsten gehen derzeit Beschwerden bei Watchlist Internet zu Phishing ein. Kriminelle versuchen, sich Passwörter oder persönliche Daten zu „angeln", etwas, das es inzwischen nicht mehr nur per E-Mail, sondern auch per SMS und Telefonanruf gibt. „Daneben sind Fake-Shops, bei denen man bestellt, bezahlt und nichts oder nur minderwertige Ware bekommt, immer noch ein Problem", sagt Behrens. „Beim Anlagebetrug gibt es zwar nicht so viele Beschwerden, dafür gibt es dort die größten Schadenssummen. Besonders dreist finden wir es, wenn uns Kriminelle eine E-Mail senden und uns mitteilen, dass ihr Angebot seriös ist und wir unsere Warnung ganz schnell von unserer Seite löschen sollen. Darüber müssen wir oft lachen", sagt Behrens.

Anzeigen. Dem Bundeskriminalamt sind 2023 über 1.700 Anzeigen wegen Fake-Shops bekannt geworden. Weitaus höher waren die Zahlen der Anzeigen wegen Bestellbetrugs (9.900) und Phishing (9.400). Der Gesamtschaden bei den angezeigten Fake-Shop-Fällen belief sich auf zumindest 1,83 Millionen Euro. Bei den 3.100 Anzeigen wegen Anlagebetrugs entstand ein Schaden von ca. 79 Millionen.

Neue Zielgruppen. Durch Fallen, die über SMS oder WhatsApp verbreitet werden, sind jetzt auch Personen betroffen, die nicht im Internet aktiv sind. Nachrichten wie „Hallo Mama, ich habe mein Handy kaputt gemacht. Meine Sim war auch kaputt, ich kann nicht viel tun, aber kannst du mir eine WhatsApp schreiben 4367764729517" sind betrügerisch. Wer die neue Nummer anrufen will, wird nie jemanden erreichen. Es folgen lediglich Ausreden, weshalb das Telefonieren nicht möglich sei.

Wie man den Betrug schnell entlarvt? „Rufen Sie Ihr Kind unter der gewohnten Nummer an oder schreiben Sie ihm eine Nachricht. Ihr Kind weiß nichts von einer angeblichen neuen Nummer", sagt Behrens. „Oder stellen Sie Ihrem Gegenüber Fragen, die nur Ihr echtes Kind beantworten könnte."

Wurde bereits Geld überwiesen, rät Watchlist Internet zu einer polizeilichen Anzeige. Hier findet ein regelmäßiger Austausch mit Bediensteten verschiedener Abteilungen im Bundeskriminalamt und in den Landespolizeidirektionen zu aktuellen Entwicklungen im Internetbetrug statt.

Wichtig ist Bewusstseinsschaffung in der Bevölkerung, um Fallen rechtzeitig erkennen zu können.

Die Tipps von Thorsten Behrens: „Wenn etwas zu gut klingt, um wahr zu sein, wäre ich auf jeden Fall einmal skeptisch. Generell schadet ein Blick ins Impressum nie, um herauszufinden, mit wem man es eigentlich zu tun hat. Gibt es kein Impressum oder ist es nicht plausibel, wäre ich auf jeden Fall vorsichtig. Vor allem, wenn es um eine Geldanlage geht, würde ich nichts investieren, wenn ich nicht klar herausfinden kann, welches Unternehmen dahintersteht. Bei einer Internetsuche zu der Webseite oder dem Anbieter findet man vielleicht Erfahrungsberichte anderer oder auch die Warnungen der *Watchlist Internet,* die einem weiterhelfen können."

Websites überprüfen. Beim Heizsystem EquiWarm Pro wird einem auf der Website equiwarmproheater.shop sogar eine ausgezeichnete Bewertung des Unternehmens mit 4,9 von 5 Sternen vorgegaukelt. Anders als üblich, ist ein Klick auf die Bewertungen aber nicht möglich – und das hat aus Sicht der angeblichen Firma auch einen guten Grund: Denn tatsächlich wird der Online-Shop mit einem Rating von nur 1,4 von 5 Sternen bewertet.

Künstliche Intelligenz für Betrüger. „Bei Nachrichten, wie der „Hallo-Mama"-Falle, die über die privaten Kanäle wie SMS oder WhatsApp kommen, würde ich auf jeden Fall über einen anderen Kanal, z. B. per Anruf, überprüfen, ob das Geschriebene stimmen kann", sagt Behrens. Auch hier heißt die Zukunft für kriminelle Banden künstliche Intelligenz (KI). Nicht nur, dass Formulierungen und Übersetzungen besser werden, gibt es nun auch erste Deepfake-Videos, in denen Prominenten Werbung für Fake-Angebote in den Mund gelegt wird.

„In nicht allzu ferner Zukunft werden wir es auch mit KI-generierten Stimmen oder Videos z. B. der eigenen Kinder oder Enkel zu tun haben", sagt Behrens. „Dann klingt der Anrufer zwar wie das eigene Kind, in Wahrheit rufen aber Betrüger an, die versuchen, Geld zu ergaunern. Bei solchen Fallen ist es wichtig, dass man sich vorher damit beschäftigt und etwa mit den Kindern ein ‚Passwort' vereinbart, mit dem man überprüfen kann, ob da wirklich das eigene Kind anruft."

Wer bereits in eine Betrugsfalle getappt ist, sollte auf jeden Fall sofort versuchen, eventuell getätigte Zahlungen zurückzubekommen. „Gerade bei Banküberweisungen ist das aber fast nicht möglich, da Überweisungen inzwischen sehr schnell an die Empfängerbank übermittelt werden und dann nicht mehr zurückgeholt werden können. Wer persönliche Daten oder gar Ausweiskopien übermittelt hat, hat keine Chance, dass die Daten wieder gelöscht werden. Wer Opfer von Internetbetrug wurde, sollte auf jeden Fall Anzeige bei der Polizei erstatten. Nur so besteht die Chance, dass die Täter gefasst und verurteilt werden können."

Julia Brunhofer/Herbert Zwickl