

Einladung zur
Bürgersprechstunde
mit Martina Machulla MdL

Donnerstag, 21. November, 16 - 17 Uhr

Café Anna Blume
Stöckener Str. 68, 30419 Hannover

Keine Anmeldung nötig!

Neue Betrugsmasche: „Pig Butchering“

Mithilfe von täuschend echter Werbung und Fake-Profilen erleichtern **CYBERKRIMINELLE** weltweit ihre Opfer um Milliarden

VON BEN KENDAL

BERLIN. Was haben ein „Tageschau“-Beitrag über die Fluggesellschaft Lufthansa und eine junge Frau namens Jessica gemeinsam? Sie sind beide nicht

real. Besagter Beitrag kursierte in den sozialen Medien. Darin hieß es: Bürgerinnen und Bürger könnten durch ein ganz bestimmtes Investment in Lufthansa viel Geld verdienen. Doch dabei handelte es sich – ermöglicht durch Künstliche Intelligenz (KI) – um einen Deepfake, der Menschen in betrügerische Investments locken sollte.

Hinter dem Social-Media-Profil der attraktiven Jessica, die vor einigen Monaten einen BBC-Reporter reinlegen wollte, steckt in Wahrheit eine Tätergruppe, die vermutlich aus China stammt. Sie verwendete Bilder vom Social-Media-Profil einer deutschen Influencerin, um den Journalisten per Instagram zu verführen und zu hohen Geldzahlungen zu bewegen. Die zwei Fälle haben noch eine Sache gemeinsam: Sie sind Teil einer großen Betrugsmasche, die als „Pig Butchering“, als Schweineschlachtung, bekannt ist.

Kriminelle Gangs nutzen die Methode, um durch Manipulation Vertrauen zu Menschen aufzubauen, sie in betrügerische Investments zu locken – und anschließend ihr Geld abzuzocken. „Die Täter haben ganze Listen mit psychologischen Tricks“, sagt Ondrej Kubovic, IT-Sicherheitsexperte bei der Firma Eset. „Sie wissen, wie sie ihre Opfer

zunächst zu kleinen Zahlungen zwingen – nur, um sie nach und nach zu mästen.“ Sie manipulieren Menschen, damit diese vertrauliche Informationen preisgeben oder ihnen Geld schicken. Sobald die Kriminellen Vertrauen aufgebaut haben, legen sie ihren Opfern ein Investment nahe.

Wer sich auf das Investment einlässt, bekommt von den Tätern klassischerweise Screenshots mit vermeintlichen Profiten. „Damit versuchen sie, ihren Opfern zu zeigen: Wenn du noch mehr investierst, bekommst du noch mehr zurück“, erläutert Kubovic. Aus diesem Prinzip leitet sich auch der Name „Pig Butchering“ ab: Die Kriminellen mästen ihre Opfer so lange mit Gewinnversprechen, bis sie sie finanziell völlig ausschachten können.

Pig Butchering-Opfer erkennen den Betrug meist erst dann, wenn sie ihr Geld aus dem Investment zurückverlangen. Die Täter fordern dazu dann den Ausweis oder Reisepass, um den Profit aus dem vermeintlichen Investment ausschütten zu können. Doch das machen die Be-

trüger nur, um die Dokumente zu missbrauchen – sie haben nie vorgehabt, ihren Opfern das Geld zurückzugeben. Für Betroffene ist es dann schon zu spät.

Betroffene können den Schaden dennoch begrenzen. Als Beweise können finanziell Geschädigte Chatprotokolle sichern und der Polizei vorlegen. Jedoch genügt das in den allermeisten Fällen nicht, um die Täter aufzuspüren. Trotzdem ist es sinnvoll, so Kubovic, Anzeige zu erstatten. Im nächsten Schritt ist es wichtig, einen weiteren Missbrauch des eigenen Geldes und der persönlichen Daten zu verhindern. Wer Tätern zum Beispiel Passwörter zu wichtigen Onlinekonten verraten hat, sollte diese unbedingt schnell ändern. „Wenn man den Kriminellen seinen Ausweis oder Reisepass geschickt hat, sollte man dies zudem melden und neue Dokumente anfertigen lassen. Die Identität kann ansonsten missbraucht werden“, sagt Kubovic.

Auch wenn Pig Butchering global ein zunehmendes Problem wird, können sich Men-

schen vor der Betrugsmasche schützen. „Die Quintessenz: Vertrauen Sie niemals jemandem, den Sie nicht kennen und der angibt, ein Experte zu sein und ihnen durch eine unverzichtbare Investment-Möglichkeit zu Geld verhelfen kann“, sagt FBI-Agent William J. DelBagno auf der Website der US-amerikanischen Sicherheitsbehörde.

Eset-Mitarbeiter Kubovic betont, dass kritisches Denken wichtig ist. Gerade die Onlineinteraktionen mit Unbekannten, die zu verlockend sind, um wahr zu sein, solle man hinterfragen. „Kriminelle geben sich oft unheimlich viel Mühe, um ihre Betrugsmasche als echtes Business zu verkaufen: Sie bauen Websites, kreieren mithilfe von KI täuschend echt aussehende Fake-Videos mit vorgegaukelten Kundenreferenzen“, sagt der Experte. Beim Onlinedating rät er Menschen dazu, über neue Kontakte mit Freundinnen oder der Familie zu sprechen. Gerade dann, wenn der Kontakt plötzlich persönliche Informationen fordert oder mit Investments lockt. „Manchmal sehen vertraute Menschen Warnzeichen, die man selbst gar nicht erkennt, weil man sich von den vielen Komplimenten geschmeichelt fühlt“, sagt Kubovic.



Verlockende Investment-Angebote sollte man sehr kritisch prüfen.

Symbolfoto: Anna Nekrashevich / Pexels

MODEZENTRUM HANNOVER

Es geht weiter im

TOTAL-AUSVERKAUF

wegen Geschäftsaufgabe

50%

RABATT AUF DIE NICHT REDUZIERTE WARE

30%

RABATT AUF DIE BREITS REDUZIERTE WARE

KRESS Modezentrum Hannover

Einkaufspark Klein-Buchholz | Sutelstr. 5

Mo - Sa 9.00 - 19.00 Uhr

Follow us

KRESS Kunden parken kostenlos direkt am Geschäft

www.kress-mode.de

HAZ

DIE 5 WICHTIGSTEN THEMEN FÜR DEINE REGION

Als Newsletter morgens in deinem Postfach.

Hier anmelden

Fünf Themen in fünf Minuten informiert für den Tag

Wissen, was Deutschland und die Region bewegt.

Hannoversche Allgemeine HAZ

rnd

Partner im RedaktionsNetzwerk Deutschland