KONSUM & MEHR

Über Geld sprechen

Frauen sollten Gehalt thematisieren

Wenn es im Bewerbungsgespräch um das Gehalt geht, sollten sich insbesondere Bewerberinnen gut vorbereiten. Denn häufig kommt die Frage: Was haben Sie in ihrem letzten Job verdient?

Genau das kann zur Falle für Frauen werden, die bislang in einem eher schlechter bezahlten Arbeitsverhältnis sind. Wenn das die Benchmark bilde, reproduziere sich die Ungleichheit im nächsten Job, sagt Rea Eldem, Geschäftsführerin von In-Visible. Ihre Agentur beschäftigt sich mit gendergerechter Arbeitskultur.

Um den Kreislauf zu durchbrechen, rät Eldem, „das offen zu thematisieren – und zu fragen, was das jeweilige Unternehmen dafür tut, geschlechtsspezifische Ungleichheiten in Sachen Gehalt zu verhindern".

Wichtig sei, dass sich Frauen auf ein solches Gespräch gut vorbereiten. Dazu gehört Eldem zufolge auch, im vertrauten Rahmen über Geld und Verdienstmöglichkeiten zu sprechen. So schaffen Frauen sich gedanklich einen neuen Referenzrahmen und trauen sich daher eher zu fordern, was ihnen zusteht. dpa

DAS URTEIL

Für den Job geeignet

Gesundheitliche Probleme dürfen nicht automatisch zur Ablehnung einer Bewerbung führen. Der potenzielle Arbeitgeber muss prüfen, ob er durch angemessene Vorkehrungen am Arbeitsplatz eine Gleichstellung erreichen kann. Das geht aus einer Eilentscheidung des Arbeitsgerichts Erfurt hervor.

Bei einer Behörde des öffentlichen Dienstes hatte sich eine Frau beworben. Nach dem Vorstellungsgespräch war klar, dass sie als Bürokauffrau fachlich geeignet ist. Die Frau hatte ein angeborenes Augenzittern – auch Nystagmus genannt. Die Behörde holte das Gutachten einer Betriebsärztin ein. Bedenken an der Eignung der Frau wurden geäußert.

Gleichzeitig gab die Betriebsärztin aber die Empfehlung: den Arbeitsplatz mit einer Bildschirmlupe, einem großen Monitor und Sehhilfen auszustatten sowie individuelle Bildschirmpausen zu ermöglichen. Die Frau war im Besetzungsverfahren als einzige fachlich geeignete Bewerberin übrig geblieben. Und so klagte sie vor Gericht.

Mit Erfolg. Im Eilverfahren bekam die Klägerin Recht. Das Arbeitsgericht ordnete die Fortsetzung des Stellenbesetzungsverfahrens an. Bereits die Untersuchung sei unzulässig gewesen.

Die Bewerbung der Klägerin wegen ihrer Sehbehinderung abzulehnen, stellt eine Benachteiligung dar. dpa
AZ.: 7 Ga 6/23

Warum Misstrauen schützt

Betrügerinnen und Betrüger versuchen über E-Mails, SMS und Anrufe an Passwörter und Bankdaten zu kommen. Stress bei den Opfern soll zu unüberlegtem Handeln führen

VON MECHTHILD HENNEKE


MORITZ WIENERT

Sehr geehrter Kunde, wir möchten Sie dringend darüber informieren, dass sofortiger Handlungsbedarf erforderlich ist", steht in der E-Mail, die angeblich von der Hypovereinsbank stammt. Es wird behauptet, dass eine Aktualisierung der Anwendung nötig sei, sonst könne es zu einer Sperrung der Online-Dienste kommen. Darunter steht ein Link, den man anklicken soll. Die E-Mail wurde von einem aufmerksamen Empfänger an die Verbraucherzentrale NRW gesandt. „Banken stehen im Fokus der Kriminellen", sagt David Riechmann, Rechtsanwalt bei der Verbraucherzentrale NRW. Betrugsversuche durch falsche E-Mails, sogenanntes Phishing, sind inzwischen bekannt. Doch es gibt weitere Maschen. Fachleute klären auf und geben Tipps, wie man vermeiden kann, in die Falle zu tappen.

Phishing, Smishing und Vishing: Drei Varianten des Betrugs, die alle mit dem Ziel eingesetzt werden, an die Passwörter des Opfers zu gelangen. „Beim Phishing werden E-Mails vermeintlich von der Sparkasse, der Postbank, Volksbank, aber auch von Paypal oder Amazon geschickt", sagt Riechmann. Der Grund: Die Betrüger versuchen über die großen Kreditunternehmen oder Online-Plattformen möglichst viele Opfer anzusprechen. In der E-Mail fordern sie dazu auf, sich auf einer betrügerischen Webseite mit den Kundendaten zu registrieren. „Mit diesen Daten plündern sie dann die Konten der Opfer", sagt Riechmann.

Beim Smishing kommt der Betrugsversuch per SMS. „Ihre Lieferung wird derzeit zurückgehalten. Verfolgen Sie sie hier: HermesLieferung.com" lautete beispielsweise eine SMS, die kürzlich an viele Handys ging. Den Link anzuklicken, hätte vermutlich dazu geführt, dass ein Virus auf dem Telefon installiert worden wäre, oder der Empfänger hätte Daten auf einer betrügerischen Webseite eingeben sollen. Riechmann rät, solche SMS zu löschen, am besten, ohne darauf zu tippen und die SMS zu öffnen.

Vishing geschieht per Telefon. Handy oder Festnetztelefon klingeln – häufig mit einer deutschen Nummer und ein Anrufer bietet an, vermeintlich wichtige Sicherheitsprobleme zu lösen. „Die Anrufer wirken oft vertrauenswürdig", sagt Margit Schneider, Direktorin des Bereichs Sicherheitsmanagement für Zahlungskarten bei der Euro Kartensysteme, einem Gemeinschaftsunternehmen der deutschen Kreditwirtschaft. „Auf Einwände und Zweifel reagieren die Betrüger mit glaubwürdigen und verständlichen Argumenten", sagt Schneider. Ein Szenario ist, dass behauptet wird, mit der Girocard hätten auffällige Transaktionen stattgefunden, wie mehrere Umsätze in Portugal in Höhe von 1200 Euro. Die Opfer sollen ihr Konto sofort prüfen über einen Link, zum Beispiel per SMS. „Dabei entlocken die Betrüger ihnen sensible Daten."

Riechmann erklärt, dass bei den Opfern bewusst Druck aufgebaut wird. „Unter Druck denken die Leute nicht, fragen nicht nach", sagt er. Eine Aussage wie „Ihr Kontozugang wurde gesperrt" löse Angst aus und verleite dazu, die Zugangsdaten preiszugeben. Jemanden so zu manipulieren, dass er oder sie bereit ist, einem Fremden persönliche Daten zu übermitteln, nennt man „Social Engineering" – deutsch etwa: soziale Steuerung. Der altbekannte Enkeltrick ist ein weiteres Beispiel dafür.

Gefahren durch Künstliche Intelligenz: KI-Programme machen manchen Betrugsversuch noch schwerer durchschaubar. So lassen sich mit KI-Software Stimmen reproduzieren, mit denen dann Vishing-Anrufe getätigt werden. „Mit den Stimmen ihrer vermeintlichen Kinder werden Eltern angerufen und gesagt, der Sohn oder die Tochter sei am Apparat und er oder sie sei in Bedrängnis", sagt Schneider. In solchen Situationen geben Eltern nicht selten Daten preis oder händigen Mittelsmännern der Betrüger direkt Geld aus.

KI-Anwendungen helfen den Phishing-Betrügern zudem, ihre E-Mails von Fehlern zu befreien. „Früher konnte man Fake-Mails oft daran erkennen, dass die Rechtschreibung falsch war, zum Beispiel die Groß- und Kleinschreibung. Das hat sich geändert. Die E-Mails sind inzwischen in korrektem Deutsch verfasst", sagt Riechmann. Und noch eine Täuschung wird durch KI ermöglicht: „Die Telefonnummern, von denen die Betrüger anrufen, sind häufig nicht echt", so Riechmann.

Abwehr von Betrugsversuchen: Grundsätzlich sollte man sich durch E-Mails, Anrufe oder SMS nicht unter Druck setzen lassen, sondern sich trotz des Stresses bremsen und gut nachdenken, rät Riechmann. „Man sollte sich fragen: Macht es Sinn, was hier steht? Was mache ich gerade eigentlich? Will ich das wirklich?", nennt er als hilfreiche Kontrollfragen. Schnelles Handeln sei gefährlich. „Ich rate zu einem gesunden Misstrauen", sagt er.

Beim Online-Kauf rät Riechmann dazu, unbekannte und möglicherweise verdächtige Shops bei einem „Fake Shop-Finder" der Verbraucherzentrale kontrollieren zu lassen (www.verbraucherzentrale.de/fakeshopfinder). Die Software prüft zum Beispiel, wie lange der Shop am Markt ist, wie seine Bewertungen sind und ob es ein reguläres Impressum gibt.

Wichtige Schritte im Schadensfall: Kommt es doch dazu, dass sensible Daten wahrscheinlich an Betrüger übermittelt wurden, tut schnelles Handeln Not. „Die Hotline 116116 kann man zu jeder Tages- und Nachtzeit anrufen", sagt Schneider. Es gibt zudem eine Sperrnotruf App („Sperr App"). Sie ist ein Service des Sperr-Notrufs. Über sie können Bankkunden Debitkarten, Kreditkarten und elektronische Zugänge automatisiert sperren – vorausgesetzt, das eigene Kreditinstitut beteiligt sich an der Sperr-App.

„Außerdem ist es sinnvoll, bei der Polizei Anzeige zu erstatten", sagt Schneider. Was viele nicht wissen: „Die Polizei kann zusätzlich die Karte für das Lastschriftverfahren sperren." Es ist weiter aktiv, auch wenn die Karte nicht mehr mit PIN genutzt werden kann. Das digitale Lastschriftverfahren tritt dort in Kraft, wo Menschen an der Kasse den Girocard-Beleg unterschreiben müssen.

Digitalführerschein: Wer überprüfen möchte, ob er oder sie im Umgang mit digitalen Herausforderungen fit ist, kann unter difue.de einen Test machen. Der Digitalführerschein (Difü) ist ein Weiterbildungs- und Zertifizierungsangebot der Bundesregierung, das den Stand der individuellen digitalen Kompetenz zeigt. Im Lernbereich gibt es praktische Tipps und Hintergrundwissen zu Fragen wie: Wie schütze ich mich vor Schadsoftware? Wie nutze ich soziale Medien sicher? Wie kann ich echte von gefälschten Nachrichten unterscheiden?