Presseinformation

KFV warnt vor KI-unterstützten Betrugsmaschen: „Jeder erlebt irgendwann einen Online-Betrugsversuch“

Gestern steckte künstliche Intelligenz noch in den Babyschuhen, heute revolutioniert sie viele Bereiche unseres Lebens. Ihre Verfügbarkeit bringt allerdings nicht nur Chancen, sondern auch erhebliche Risiken mit sich. Wie die neueste Studie - eine Kooperation des KFV Fachbereichs Eigentumsschutz und der Watchlist Internet - zeigt. Der Einsatz von KI in Betrugsmaschen ist besorgniserregend. Von klassischen Phishing-Attacken bis hin zu hochentwickelten KI-gestützten Täuschungen: Die dramatische Entwicklung einer facettenreichen Form von Internet-Kriminalität schreitet weiterhin rasant voran.

Wien, 25. November 2024. Die Evolution des Online-Betrugs ist beunruhigend. Eine aktuelle KFV-Umfrage von 1.033 Teilnehmenden im Alter zwischen 14 und 75 Jahren zeigt: 83 Prozent der Befragten gaben an, in den letzten 12 Monaten Betrugsversuche bemerkt zu haben. Dabei handelt es sich nur um die Spitze des Eisberges, denn viele Betrugsversuche bleiben unbemerkt. „Es ist davon auszugehen, dass nahezu jede*r Internetnutzer*in irgendwann einem Betrugsversuch ausgesetzt ist, selbst wenn dieser nicht bewusst wahrgenommen wird oder man nicht darauf hereinfällt. Oftmals werden solche Versuche direkt in Spam-Ordnern abgefangen oder als verdächtige Nachrichten in Messengerdiensten gelöscht,“ erklärt **Dr. Armin Kaltenegger, Leiter des Fachbereichs Eigentumsschutz im KFV**.

Die häufigsten Kontaktwege, über die Betrugsversuche im Internet passieren, finden per E-Mail statt (68 %), dicht gefolgt von Kurzmitteilungen, also sogenannten SMS (60 %) und Telefonanrufen (50 %). Bemerkt wurden vor allem Betrugsversuche wie Phishing (64,8 %), Gewinnspielbetrüge (50,4 %), Investitionsbetrüge (25,8 %), Fake-Shops (25,1 %), falsche Rechnungen (24,8 %) sowie der sogenannte Enkeltrick (24,5 %).

Phishing gehört tatsächlich zu den häufigsten Formen des Online-Betrugs. Es handelt sich dabei um einen Versuch, über gefälschte E-Mails, Webseiten oder Nachrichten persönliche Daten wie Passwörter oder Kreditkartendaten zu stehlen. Auch Investmentbetrug verbreitet sich immer mehr. Hiermit handelt es sich um eine raffinierte Form des Betrugs, bei der Kriminelle gezielt Vertrauen aufbauen, um ihre Opfer zu einer Investition zu verleiten. Aber auch betrügerische Online-Shops sind ein wachsendes Problem, das sowohl finanzielle Schäden als auch den Verlust persönlicher Daten zur Folge haben kann. „Wir beobachten aktuell eine starke Professionalisierung im Internetbetrug. Durch Phishing-Attacken und zum Teil auch per Fake-Shop werden Daten über potenzielle Opfer gesammelt. So können Kriminelle ihre Opfer viel persönlicher ansprechen und Vertrauen aufbauen, das dann dazu missbraucht wird, um deutlich höhere Beträge zu ergaunern,“ erklärt **Thorsten Behrens, Projektleiter Watchlist Internet**.

SAFETY FIRST!

Jede fünfte befragte Person Opfer eines Betrugs im Internet
20 Prozent der Befragten haben einen Online-Betrug bereits selbst erfahren müssen. Dabei waren Männer häufiger betroffen als Frauen. „Von einem Datenleck oder einer Datenpanne waren sogar 22 Prozent betroffen und 5,5 Prozent der Befragten gaben an, bereits Opfer eines KI-unterstützten Betrugs gewesen zu sein. Dabei schätzen mehr als zwei Drittel ihr Wissen über Betrugsmaschen als sehr gut oder zumindest eher gut ein," so **Kaltenegger**. Auch wenn man sich an die bisherigen Betrugsversuche bereits gewöhnt hat, haben sich durch die KI neue Möglichkeiten des Betrugs ergeben, die den „Lernfortschritt" wieder ausgleichen. Die neuen, KI-gestützten Tricks sind sogar für vorsichtige und informierte Personen oft schwer zu erkennen. Häufig nutzen die Kriminellen den Moment der Unachtsamkeit oder der emotionalen Verletzlichkeit, um ihre Opfer unter Druck zu setzen - und ihre Methoden werden durch den Einsatz von künstlicher Intelligenz immer raffinierter.

KI-gestützte Täuschungen
Die Betrüger sind erfinderisch und passen sich schnell an neue Technik an: KI-unterstützte Betrugsmaschen nutzen fortschrittliche Technologien wie Deepfakes und Voice Cloning, um Menschen zu täuschen und zu manipulieren. Diese neuen Methoden sind besonders gefährlich, da sie schwer zu entlarven sind und das Vertrauen der Opfer gezielt ausnutzen. Durch den Einsatz einer vertraut klingenden Anrede, gefälschter Telefonnummern, die eine bekannte Nummer anzeigen lassen - etwa die eines Krankenhauses, einer Behörde oder einer Familiennummer - aber auch durch KI-gestützte Sprachsynthese-Techniken, die Stimmen von Familienmitgliedern oder Freund*innen des Opfers imitieren, wird es den Kriminellen ermöglicht, in die Rolle einer vertrauten Person zu schlüpfen.

Zusätzlich ermöglicht KI emotionale Manipulationstechniken genauer abzustimmen und auf das Verhalten und die Reaktionen des Opfers anzupassen. Indem das System auf bestimmte Antworten und Emotionen reagiert, kann es das Gespräch in Echtzeit dynamisch verändern und genau die Informationen liefern, die das Opfer emotional beeinflussen und unter Druck setzen. So wird es für die Opfer immer schwieriger, zwischen einem echten Hilferuf oder einer authentischen Nachricht und einem gut ausgeklügelten Betrug zu unterscheiden.

Präventionstipps: So kann man sich vor KI-Betrug schützen
Zwei von drei Befragten (66 %) gaben an, von KI-unterstützten Betrugsversuchen bereits gehört zu haben. Dies zeigt, dass das Bewusstsein für diese neue Form des Betrugs in der Bevölkerung wächst. Doch gleichzeitig werden die Online-Betrügereien auch immer raffinierter und ausgefeilter. Deshalb ist es wichtig, dass sich auch die Präventionsmaßnahmen und die Wachsamkeit der potenziellen Opfer kontinuierlich weiterentwickeln.

Folgende Präventionsmaßnahmen sorgen für mehr Sicherheit:

1. **Seien Sie skeptisch**: Wenn etwas zu schön klingt, um wahr zu sein, ist es das wahrscheinlich auch. Dies gilt besonders für unerwartete Angebote, Gewinne oder dringende Anfragen.
2. **Überprüfen Sie Quellen, Absender und Links**: Klicken Sie nicht voreilig auf Links in E-Mails oder SMS. Überprüfen Sie sorgfältig die Absenderadresse und seien Sie vorsichtig bei unbekannten oder verdächtigen Absendern. Folgen Sie nie dem Link, sondern überprüfen Sie direkt im Konto des jeweiligen Anbieters (Website oder App) ob tatsächlich eine Aktion notwendig ist.
3. **Schützen Sie Ihre persönlichen Daten**: Geben Sie keine vertraulichen Informationen wie Passwörter, Kreditkartendaten oder TANs preis, besonders nicht am Telefon oder in E-Mails.
4. **Nutzen Sie starke Authentifizierung**: Aktivieren Sie die Zwei-Faktor-Authentifizierung, wo immer möglich. 61 Prozent der Befragten, die aktiv Präventionsmaßnahmen ergriffen haben, nutzen diese Methode.
5. **Halten Sie Ihre Software aktuell**: Führen Sie regelmäßig Sicherheits-Updates durch. Die KFV-Studie zeigt: 50 Prozent der Befragten nutzen derartige Updates als Schutzmaßnahme.
6. **Verwenden Sie unterschiedliche Passwörter**: Nutzen Sie nicht das gleiche Passwort für alle Konten. 54 Prozent der Befragten befolgen diesen Rat bereits.
7. **Seien Sie vorsichtig bei Online-Shops**: Überprüfen Sie das Impressum, die Zahlungsmethoden und die Preise. Wenn etwas zu günstig erscheint, könnte es sich um einen Fake-Shop handeln.
8. **Bleiben Sie informiert**: Halten Sie sich über aktuelle Betrugsmaschen auf dem Laufenden. Nutzen Sie vertrauenswürdige Quellen wie die Watchlist Internet.
9. **Reagieren Sie richtig auf Datenlecks**: Wenn Sie von einem Datenleck betroffen sind, ändern Sie umgehend Ihre Passwörter. 68 Prozent der Betroffenen haben dies getan.
10. **Seien Sie besonders wachsam bei KI-gestütztem Betrug**: Denken Sie daran, dass Stimmen und Videos gefälscht sein können. Verifizieren Sie wichtige Informationen immer über einen zweiten, vertrauenswürdigen Kanal. Achten Sie auf kleine Verzögerungen oder unnatürliche Bewegungen bei Videos.
11. **Teilen Sie Ihr Wissen**: Informieren Sie Freund*innen und Familie über neue Betrugsmaschen. Gemeinsam können wir ein Netzwerk der Prävention aufbauen.
12. **Vertrauen Sie Ihrem Instinkt**: Wenn Sie ein ungutes Gefühl haben, nehmen Sie sich die Zeit, die Situation genau zu überprüfen. Lassen Sie sich nicht unter Druck setzen.
13. **Bei unerwarteten Anrufen misstrauisch sein**, beenden Sie das Gespräch und rufen Sie den vermeintlichen Verwandten unter seiner bekannten Telefonnummer zurück. Es kann auch ein geheimes Codewort oder eine Kennfrage vereinbart werden.
14. **Gespräch unterbrechen und Hilfe holen**: Wenn ein Anrufer Sie unter Druck setzt, sollten Sie das Gespräch sofort beenden und eine Vertrauensperson zurate ziehen. Führen sie keine Geldübergaben an Dritte durch, kontaktieren Sie im Zweifelsfall die Polizei.

Link zur Aufzeichnung der Pressekonferenz

Fotos, Abdruck honorarfrei

Dr. Armin Kaltenegger, Leiter des Bereichs Eigentumsschutz im KFV © KFV/APA Fotoservice/Schedl

Thorsten Behrens, Projektleiter Watchlist Internet ©ÖIAT/Summereder

Fotos der Pressekonferenz © KFV

Rückfragehinweis:
Pressestelle KFV (Kuratorium für Verkehrssicherheit)
Tel.: 05-77077-1919 I E-Mail: pr@kfv.at I www.kfv.at