Bundesministerium
Inneres

Bundeskriminalamt

KFV

Presseinformation

KI-Betrugsdelikte: So schützt man sich vor Kriminellen

Die Anzahl der Betrugsdelikte im Internet steigt. Gründe dafür sind die zunehmende Internetnutzung und der technologische Fortschritt. Derzeit stellt Künstliche Intelligenz (KI) eine neue Herausforderung dar. Aufklärung der Bevölkerung und Prävention mittels technischer Hilfsmittel zählen aber auch in diesem Bereich zu den effektivsten Vorsichtsmaßnahmen. In einer gemeinsamen Pressekonferenz zeigten Bundeskriminalamt, KFV und ein KI-Experte, welche Täuschungsmanöver mittels KI bereits jetzt schon möglich sind und wie sich die Bevölkerung generell vor Betrügern schützen kann. Zudem wird erklärt, welche KI-Anwendungen legal sind und wann man sich strafbar macht.

Wien, 17. November 2023. Cybercrime boomt. Im Jahr 2022 sind die angezeigten Straftaten im Bereich der Internetkriminalität um 30 Prozent auf mehr als 60.000 gestiegen. Sexualdelikte fallen da ebenso darunter wie Vermögensdelikte. Bei Betrugsdelikten gibt es ein Plus von 23 Prozent auf mehr als 27.600 Fälle und der Schaden belief sich auf 700 Millionen Euro – wobei die Dunkelziffer noch weit höher sein dürfte. „Mit ein Grund für den rapiden Anstieg ist der stetige technologische Fortschritt. Zudem agieren die Täter häufig aus dem Ausland, was die Rückverfolgbarkeit der Straftaten sowie den Zugriff auf die Täter und auf das entwendete Vermögen erschwert“, erklärt **Mag. Manuel Scherscher, Leiter der Abteilung für Wirtschaftskriminalität und Betrug im BK**.

Wer sich schützen will, sollte die Instrumente seiner Gegner kennen

Der Einsatz von Künstlicher Intelligenz (KI) spielt derzeit im Bereich der Internetkriminalität noch eine untergeordnete Rolle, aber die Entwicklung schreitet enorm voran. Aufklärung der Bevölkerung zählt daher auch in diesem Bereich zu den effektivsten Präventivmaßnahmen. „Um sich wirksam vor Deepfakes – sprich realistisch wirkenden Medieninhalten – zu schützen, sollte man wissen, welche technischen Möglichkeiten es jetzt schon gibt und wie man sich davor schützen kann“, erklärt **Dr. Sven Kurras, Director of Analytics bei RISK IDENT.** Der KI-Experte zeigte anhand praktischer Beispiele vor, dass bereits jetzt Gesichter, Stimmen, Videos und sogar ganze Dialoge künstlich erzeugt werden können, wobei diese aber derzeit teilweise noch fehlerbehaftet sind.

Praktische Tipps zum Erkennen von Deepfakes

Dr. Kurras empfiehlt insbesondere auf folgende Punkte zu achten, um Deepfakes zu enttarnen: „Unscharfe Übergänge zwischen Gesichtern und dem Hintergrund sind sehr verdächtig, ebenso asymmetrische Brillen. Wenn Teile von Bildern oder Videos eine unterschiedliche Auflösung haben, sollte man ebenfalls auf der Hut sein.“ Wichtig ist auch das Bauchgefühl: Verhält sich die andere Person untypisch? Gibt es Auffälligkeiten in der Mimik, bei den Mundbewegungen, den

Zähnen, beim Blinzeln oder der Lippensynchronität? Auch eine andere Aussprache, Betonung, Wortwahl oder Dialekt als gewohnt, können laut dem KI-Experten Alarmsignale sein.

Hat man während eines Live-Videocalls Verdacht geschöpft, könnte man das Gegenüber zu gezielten Tests auffordern, wie zum Beispiel zum Singen, um Text-To-Speech-Modelle zu entlarven. Um Face-Overlays zu stören, ist die Aufforderung die Hand vor dem Gesicht zu schwenken, ein guter Tipp. Zudem gibt es algorithmische Gegenmaßnahmen zur Deep-Fake-Erkennung. Für den Privatbereich gibt es bereits recht nützliche technische Tools, um mittels KI verfälschte Videos zu enttarnen, wie beispielsweise den Deepfake-O-Meter oder den Scanner von Deepware, wobei deren Websites zum Zeitpunkt des Versands dieser Presseaussendung gerade gewartet wurden.

Wissen über KI laut KFV-Umfrage noch begrenzt
Künstliche Intelligenz bietet allerdings nicht nur Schattenseiten, sondern auch sehr viel positives Potenzial, etwa im Bereich der Arbeitsvereinfachung und Steigerung der Effizienz. Aber auch dabei gilt es einiges zu beachten, denn nicht jeder, der sich strafbar macht, tut dies aus böser Absicht. Wie eine aktuelle Umfrage des Fachbereichs Eigentumsschutz im KFV zeigt, gaben nur knapp 10% der Befragten an, über ein umfassendes Wissen über KI zu besitzen, 52% verfügen nur über ein Basiswissen, 35% stufen ihr Verständnis als begrenzt ein und 3% gaben an, überhaupt kein Wissen in dem Bereich zu haben.

Was ist erlaubt und ab wann macht man sich strafbar?
Dr. Armin Kaltenegger, Leiter des Bereichs Eigentumsschutz sowie des Bereichs Recht und Normen im KFV erklärte, dass der Einsatz von Künstliche Intelligenz auch unbewusst und ohne böse Absichten strafbar werden kann, zum Beispiel bei der Verletzung von Urheberrechten oder dem fahrlässigen Vertrauen in KI-gesteuerte Algorithmen. Die Frage, ob intelligente Computer sogar als Täter im strafrechtlichen Sinn angesehen werden könnten, wurde von dem erfahrenen Juristen hingegen verneint: „Aufbauend auf den Prinzipien westlicher Rechtssysteme wird das nicht möglich sein“. Aber wer haftet dann für ein von KI-Systemen selbst erlerntes Fehlverhalten? Überhaupt niemand? Diejenigen, die KI-Dienstleistungen zur Verfügung stellen? Oder gar die Nutzer? Dr. **Kaltenegger** dazu: „Ob dieses Phänomen den Betreibern oder Nutzern angerechnet werden kann, wird sehr stark von der Lernfähigkeit der Systeme und der Vorhersehbarkeit der Prozesse abhängen. Ein wichtiger Faktor wird auch sein, wie die Rechtsordnung darauf reagiert“.

Etablierte Betrugsformen stellen derzeit noch immer den Großteil der Delikte dar.
Folgende Tipps sollten beachtet werden:

Bundesministerium
Inneres

Bundeskriminalamt

KFV

Neffen- und Nichtentrick

- Formulierungen wie **"Rat mal, wer da spricht!"** oder **"Erkennst du mich denn nicht?"** sollten stutzig machen. Lassen Sie sich auf kein Namen-Raten ein! Verlangen Sie, dass die anrufende Person **von sich aus** Ihren Namen nennt!
- Wenn der Name genannt wurde, stellen Sie noch eine **persönliche Frage**, die nur im **vertrauten Familienkreis** beantwortbar ist!

Falsche Polizisten

- Echte Polizisten holen niemals **Geld, Schmuck & Co.** von Privathaushalten ab, um diese sicher zu verwahren.

Datendiebstahl

- Vorsicht bei WhatsApp, SMS und E-Mails von unbekannten Absendern. Klicken Sie nicht auf unbekannte Links, öffnen oder installieren Sie keine unbekannten Dateien und Programme!

Unverlangte Werbeanrufe (Cold Calls)

- **Brechen** Sie bei unverlangten Werbeanrufen (Cold Calls) eiskalt **das Gespräch ab**! Sie haben ein Recht darauf, nicht belästigt zu werden.

Ping-Anrufe

- **Unterdrücken** Sie die Nummern von **lästigen Anrufern**!
- Rufen Sie **unbekannte Nummern** aus dem Ausland nicht zurück!

Allgemeine Tipps

- **Vorsicht bei E-Mails und Links:** Öffnen Sie keine E-Mails oder klicken Sie nicht auf Links von unbekannten Absendern.

- **Starke Passwörter und 2-Faktor-Authentifizierung:** Verwenden Sie komplexe Passwörter, die Buchstaben, Zahlen und Sonderzeichen enthalten. Aktivieren Sie eine 2-Faktor-Authentifizierung.

- **Softwareaktualisierungen:** Halten Sie Ihr Betriebssystem, Ihre Browser und Ihre Sicherheitssoftware auf dem neuesten Stand.

SAFETY FIRST!

- **Sichere Verbindungen:** Achten Sie auf das "https://" in der URL, wenn Sie sensible Informationen online übertragen. Vermeiden Sie die Nutzung von öffentlichem WLAN für vertrauliche Transaktionen.

- **Kontenüberwachung:** Überprüfen Sie regelmäßig Ihre Bank- und Kreditkartenabrechnungen, um verdächtige Aktivitäten zu erkennen.

Fotos, Abdruck honorarfrei **© KFV/APA Fotoservice/Schedl**
Fotolink: https://www.apa-fotoservice.at/galerie/35106

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