PRESSEINFORMATION

Wien, 05. Februar 2024

Europäisches Verbraucherzentrum Österreich

ECC-Net

Safer Internet Day: EVZ warnt vor aktuellen Phishing-Methoden

Künstliche Intelligenz und zunehmende „digitale Verknüpfung" erleichtern Phishing-Angriffe

In den letzten Jahren stieg die Zahl der Cybercrime-Delikte beständig – nicht zuletzt befeuert durch die COVID-19-Pandemie und die Möglichkeiten, die künstliche Intelligenz (KI) mittlerweile auch in diesem Bereich mit sich bringt. Phishing ist eine der möglichen Ausprägungen von Cybercrime, vor denen das Europäische Verbraucherzentrum (EVZ) im Verein für Konsumenteninformation immer wieder warnt. Welche Formen von Phishing aktuell häufig angewendet werden und was Betroffene tun sollten, darüber informiert im Folgenden EVZ-Juristin Maria Semrad.

Was ist Phishing?

Wurde eine offiziell wirkende Nachricht über einen unüblichen Weg zugestellt? Hat sich etwa das Finanzamt via WhatsApp gemeldet oder die Bank auf Instagram? „In derartigen Fällen können Sie davon ausgehen, dass Sie einem Phishing-Angriff ausgesetzt sind", so Maria Semrad, Juristin im Europäischen Verbraucherzentrum (EVZ) Österreich. Als Phishing-Angriffe bezeichnet man betrügerische E-Mails, Textnachrichten, Telefonanrufe oder Websites, die Betroffene zur Weitergabe vertraulicher Daten (z. B. Kreditkartennummern, Anmeldedaten) oder zum Download von Malware verleiten sollen. Dies kann zu Identitätsdiebstahl, Kreditkartenbetrug oder Ransomware-Angriffen führen, und damit auch zu herben finanziellen Verlusten.

„Problematisch ist, dass auch Cyberkriminelle zunehmend auf die Möglichkeiten künstlicher Intelligenz zugreifen", betont Semrad. „Zum Beispiel durch Voice-Cloning und Deepfakes, oder einfach durch qualitativ hochwertige Übersetzungen – wenn eine Phishing-Welle aus einem Sprachraum in einem anderen wiederholt wird. Bislang ließen sich Phishing-Versuche an Grammatik- oder Rechtschreibfehlern gut erkennen. Dies wird nun schwerer."

Spear-Phishing

Um Spear-Phishing handelt es sich, wenn individualisierte Fake-Nachrichten an eine bestimmte Personengruppe wie etwa die Mitarbeiter:innen eines Unternehmens oder die Mitglieder eines Vereins adressiert werden. Die Angreifer:innen haben detailliertere Daten der Zielpersonen, zum Beispiel aus einer geleakten Kundendatenbank, um die täuschende Nachricht mit echten Informationsbruchstücken auszustatten, sodass sie nicht ignoriert wird. Spear-Phishing-Angriffe werden angesichts der Vielzahl an Spuren, die wir als digitale Konsument:innen im Netz hinterlassen, immer häufiger.

Multi-Channel-Phishing

„Verschärft wird die Situation durch die Ausbreitung von Phishing auf neue Plattformen", so Semrad. „Je mehr Kanäle eine Privatperson abseits von E-Mails nutzt, z. B. Social Media, SMS und Apps, desto mehr Zugangspunkte ergeben sich für Kriminelle. Attacken erfolgen nun auch öfter über mehrere Kanäle gleichzeitig, da sie so glaubwürdiger scheinen." So kann zum Beispiel per E-Mail und WhatsApp eine Verständigung über Probleme mit einer Paketlieferung erfolgen samt weiterführendem Link zu einer Webseite, wo dann Zugangsdaten abgefragt werden oder das Gerät bei Download einer Datei mit Schadsoftware infiziert wird.

Romance Scams

ChatGPT, gestohlene Bilder und Videos, sowie die Tatsache, dass Social-Media-Kanäle vermehrt miteinander verknüpft werden, erleichtern es Kriminellen, Fake-Identitäten glaubwürdig und attraktiv aussehen zu lassen. Bei Romance Scams auf Social Media oder Partnerbörsen zielen Betrüger:innen üblicherweise auf „Vorschussbetrug" ab. So wird eine Beziehung vorgetäuscht, in der die Betrüger:innen erst nach einiger Zeit um Geld bitten. „Häufig geht es um Geld für ein Flugticket oder um Passgebühren, um einen persönlichen Besuch zu ermöglichen",

informiert Semrad. „Es besteht aber auch die Gefahr des Identitätsdiebstahls, indem das umschmeichelte Opfer zum Beispiel Log-in-Daten bereitstellt oder der Installation einer bestimmten Software (z. B. Anydesk) zustimmt und die Kontrolle über Programme, Konten oder das Computersystem verliert."

Tipps der EVZ-Juristin Maria Semrad:

Vorsicht ist der beste Schutz:

- Nachrichten aufmerksam und kritisch lesen, sich nicht drängen lassen und nicht vorschnell auf Aufforderungen reagieren.
- Die Angreifer:innen tarnen ihre Phishing-Attacken oft als Datenabfragen von Behörden, Telekomanbietern, Banken oder anderen bekannten Stellen. Niemals Zugangsdaten oder Passwörter weitergeben! Kein seriöses Unternehmen oder Bankinstitut fordert per E-Mail, WhatsApp oder SMS zur Eingabe von Passwörtern oder persönlichen Daten auf.
- Bei Zweifel an der Echtheit einer Nachricht besser den Kontakt mit dem „behaupteten" Absender aufnehmen. Dabei aber unbedingt die Kontaktdaten gesondert ermitteln und nicht aus der Nachricht übernehmen!

Wenn Phishing-Attacken öfter durchdringen:

- Den Computer mit einem aktualisierten Antivirus-Programm scannen, um zu sicherzustellen, dass keine Schadsoftware vorhanden ist und (noch mehr) Daten gestohlen werden können.
- Betrügerische Nachrichten immer in den Spam-Ordner des E-Mail-Programms verschieben. Das hilft, künftige Phishing-Mail-Versuche besser zu erkennen.
- E-Mail-Provider mit hohen Sicherheitsstandards nutzen. Folgende Schutzstandards sollte der E-Mail-Dienst erfüllen: SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail), DMARC (Domain-based Message Authentication Reporting & Conformance)

Falls bereits Bezahldaten auf einer Phishing-Seite eingegeben wurden:

- Kennwörter möglichst schnell ändern, vor allem, wenn bei mehreren Konten dieselben Zugangsdaten verwendet werden.
- Den betroffenen Zahlungsdienstleister kontaktieren. Überprüfen, ob schon unerwünschte Zahlungen abgeflossen sind. Bezahlkarten sicherheitshalber sperren lassen, um Schaden zu vermeiden.
- Bei Online-Zahlungsanbietern (z. B. PayPal) die Autorisierungsmethode zurücksetzen, falls das Konto kompromittiert ist.
- Falls schon Buchungen getätigt wurden, sofort eine Rückbuchung beim Kreditinstitut veranlassen.
- Ist ein finanzieller Schaden entstanden, eine Betrugsanzeige bei der Polizei machen.

In jedem Fall andere warnen, um weiteren Schaden zu verhindern:

- Sofern Zugangsdaten für Social-Media-Plattformen oder die private E-Mail-Adresse kompromittiert wurden, sollten die Kontakte der entsprechenden Accounts gewarnt werden, für den Fall, dass die Kriminellen diese Adresslisten für Folgenachrichten missbrauchen oder versuchen, diese im Namen des Geschädigten anzuschreiben.
- Falls sich die Kriminellen in der Phishing-Nachricht als Unternehmen oder öffentliche Einrichtung ausgeben, hilft es, diese Institutionen zu informieren, damit sie Warnungen an ihre Nutzer:innen aussenden können.

Zudem ist es sinnvoll, Warnportale wie die Watchlist Internet www.watchlist-internet.at oder die Meldestelle für Cybercrime im Bundeskriminalamt über den Betrugsversuch zu informieren.

SERVICE: Weitere Informationen zum Thema Phishing gibt es auf www.europakonsument.at/phishing.

RÜCKFRAGEHINWEIS FÜR MEDIENANFRAGEN: VKI-Pressestelle, Tel.: +43 664 231 44 81, E-Mail: presse@vki.at

Finanziell unterstützt durch die Europäische Union

Europäisches Verbraucherzentrum Österreich ECC-Net