Betrug zum Fest

Münster/Kaiserslautern/Gifhorn/Berlin (D).
Falsche Telekommunikationsfirmen versuchen sich Zutritt zu erschleichen. Aber auch die Internet-Käufe sowie die Nutzung von Passworten im Internethandel bergen Gefahren. Geldgeschenke sowie Anlagen werden häufig an Jugendliche, auch als Geschenk für die Zukunft gemacht. Aber Achtung, auch hier warten Fallen.

Die Polizei warnt deshalb erneut: Gewähren Sie Personen, auch wenn sie sich ausweisen, keinen unmittelbaren Zugang zur Wohnung. Sie sind nicht verpflichtet, fremde Personen hereinzulassen. Nehmen Sie sich Zeit und kontaktieren Sie Ihren Vermieter oder die Hausverwaltung, um zu klären, ob solche Vorhaben angekündigt wurden. Im Zweifelsfall empfehlen wir, keine unbekannten Personen in Ihre Wohnung zu lassen und stattdessen einen Termin zu vereinbaren.

Wenn sie einen Betrugsverdacht vermuten, wählen sie die 110. Hinweise zu verdächtigen Personen sollten immer an die örtliche Polizei erfolgen.

Dass Passwörter im gesamten Online-Geschäft eine große Rolle spielen, ist eigentlich nichts Neues. Wie wichtig es ist, mit diesen sorgsam umzugehen, wird allerdings immer noch unterschätzt.

Ein aktueller Fall aus Kaiserslautern bestätigt das: Eine 69-jährige Frau erstattete am Donnerstag Anzeige, nachdem sie per Post eine Mahnung eines Online-Versandhändlers erhalten hatte. Darin wurde eine nicht bezahlte Rechnung über einen höheren dreistelligen Betrag zu einer Bestellung aus Oktober angemahnt.

Wie die Betroffene der Polizei gegenüber angab, besitze sie zwar bei dem Versandhändler ein Kundenkonto, habe dort aber seit mindestens zwei Jahren nichts mehr bestellt. Allerdings stellte sich im weiteren Gespräch mit den Beamten heraus, dass vor ein paar Wochen das Mailkonto der 69-Jährigen gehackt worden war. Und genau diese Mailadresse war mit dem nun betroffenen Kundenkonto verknüpft.

Recherchen bestätigten den Verdacht: Die jetzt angemahnte Bestellung wurde über das Kundenkonto der Frau aus Kaiserslautern aufgegeben - aber mit einer anderen Mailadresse. Als Lieferadresse wurde ein Paketshop eingetragen. Die Hacker hatten sich also Zugang zum Konto der 69-Jährigen verschafft und die hinterlegten Daten geändert. Leider war die Dame nicht auf die Idee gekommen, nach dem gehackten Mailkonto die Zugangsdaten ihrer verknüpften Kundenkonten zu ändern.
Glück im Unglück: Der Versandhändler befreite die Frau von der Zahlpflicht. Ihr entstand also kein finanzieller Schaden. Die polizeilichen Ermittlungen wegen des Betrugs dauern an.

Unsere Empfehlung:
Sorgen Sie für einen stärkeren Schutz Ihrer Online-Konten. Viele Plattformen bieten neben den üblichen Zugängen über Benutzername und Passwort auch eine sogenannte Zwei-Faktor-Authentifizierung an. Sie sorgt dafür, dass bei einem Login-Versuch zusätzlich ein Code zum Beispiel an eine hinterlegte Handynummer verschickt und der Zugang erst freigegeben wird, wenn die angezeigte Kombination aus Zahlen und Buchstaben eingetippt wird.

Weitere Informationen zu diesem Thema finden Sie im Internet auf der Seite www.polizei-beratung.de

Gern werden zu Weihnachten auch Geld oder Anlagen verschenkt. Folgendes Beispiel sollte jeden vor dem Geschäft:
Hier ein Beispiel: Ein Mann aus dem Landkreis Kusel ist Opfer eines Online-Anlagebetrugs geworden. Wie der 64-Jährige über die Onlinewache der Polizei Rheinland-Pfalz meldete, war er im Oktober auf einer Social-Media-Plattform auf eine Werbeanzeige aufmerksam geworden, die Anlagegeschäfte mit Kryptowährungen anbot. Der Mann wurde neugierig und klickte die verlinkte Seite an. Dort legte er sich ein Zugangskonto an, bei dem er seine kompletten personenbezogenen Daten angab und auch ein Passfoto hochlud.

In der Folge kam es zu mehreren Telefonaten mit angeblichen Anlageberatern. Dabei gewährte der 64-Jährige den Unbekannten per Fernzugriff den Zugang zu seinem Laptop, um ein notwendiges Programm für den Online-Handel zu installieren und ihm dieses zu erklären.

Nachdem erste Investitionen in seinem Onlinekonto als sehr erfolgreich angezeigt wurden, entschloss sich der Mann zu weiteren Überweisungen. Erst als er bei einer eigenen Internet-Recherche zu der genutzten Plattform auf Einträge stieß, die von Betrugsfällen berichteten, kamen dem 64-Jährigen Zweifel, ob das Portal tatsächlich seriös ist. Er brach daraufhin den Kontakt zu den vermeintlichen Anlageberatern ab und informierte die Polizei. Wieviel Geld der Mann nun tatsächlich verloren hat, steht noch nicht fest.

COPYRIGHT WWW.KOMDIENST.DE REDAKTION HORST-DIETER SCHOLZ

Eine weitere Variante ist der Anlagebetrug mit Kryptowährungen

Die Polizeiinspektion Wilhelmshaven/Friesland warnt vor einer zunehmenden Zahl von Betrugsfällen im Zusammenhang mit vermeintlich gewinnbringenden Anlagen in Kryptowährungen. In mehreren bekannt gewordenen Fällen sind teils erhebliche Vermögensschäden entstanden. Nach bisherigen Erkenntnissen werden die späteren Geschädigten häufig durch professionell wirkende Werbeanzeigen im Internet auf angeblich seriöse Krypto-Handelsplattformen aufmerksam. Nach einer Registrierung erfolgt zeitnah eine telefonische Kontaktaufnahme durch vermeintliche „Broker“. Diese überzeugen die Betroffenen von der Anlagemöglichkeit und veranlassen zunächst zu einer vergleichsweise geringen Einzahlung. Durch vorgetäuschte oder tatsächlich ausgezahlte kleinere Gewinne wird Vertrauen aufgebaut. Im weiteren Verlauf werden die Geschädigten zu deutlich höheren Investitionen gedrängt. Dabei bieten die Täter Unterstützung durch Fernzugriffssoftware an, die auf den Endgeräten der Geschädigten installiert werden soll. Durch diesen Zugriff erhalten die Täter umfassende Kontrolle über Computer oder Smartphones. Die angeblichen Investitionen auf Krypto-Plattformen finden tatsächlich nicht statt; stattdessen werden die Gelder auf ausländische Konten transferiert und anschließend über Kryptowährungen verschleiert. Die eingezahlten Beträge sind in der Regel vollständig verloren. Die Polizei rät dringend zu besonderer Vorsicht und weist auf folgende Grundsätze hin: - Seien Sie grundsätzlich misstrauisch bei ungewöhnlich hohen Gewinnversprechen. - Vertrauen Sie Ihr Geld nur bekannten und überprüfbaren Anbietern an.

- Lassen Sie sich nicht unter Zeitdruck setzen.
- Sprechen Sie vor finanziellen Entscheidungen mit Vertrauenspersonen.
- Geben Sie persönliche Daten und Zugangsdaten nicht weiter.
- Gewähren Sie Unbekannten keinen Fernzugriff auf Ihre digitalen Endgeräte. Typische Warnsignale für Anlagebetrug sind unter anderem:
- Hohe Gewinne bei angeblich geringem Risiko.
- Werbeanzeigen mit prominenten Personen oder angeblichen Erfolgsgeschichten.
- Kontaktaufnahmen über soziale Netzwerke oder Dating-Plattformen.
- Sehr schnelle telefonische Betreuung nach einer Registrierung.
- Aufforderungen zur Installation von Fernzugriffsprogrammen wie TeamViewer oder AnyDesk. - Fehlende oder unvollständige Angaben im Impressum der Plattform.
- Aufforderungen zu Überweisungen auf Privatkonten.
- Auszahlungsversprechen, die an weitere Gebühren oder Steuern geknüpft sind. Zudem warnt die Polizei vor sogenannten Anschluss- oder „Recovery“-Betrügereien.

Dabei melden sich nach einem bereits erfolgten Anlagebetrug angebliche Dienstleister, die versprechen, verlorenes Geld gegen eine Gebühr zurückzuholen. Auch hierbei handelt es sich regelmäßig um Betrug. Betroffene oder Personen, die verdächtige Beobachtungen gemacht haben, werden gebeten, sich an ihre örtliche Polizeidienststelle zu wenden.

Text: Polizei Münster Polizeipräsidium Westpfalz,
Polizeiinspektion Wilhelmshaven/Friesland, Horst-Dieter Scholz