Praxistipp: Nutzen Sie die Watchlist Internet!

Topaktuelle Warnungen vor aktuellen Betrugsmaschen, die Ihre (EDV-) Sicherheit bedrohen

Seit Monaten ist die Umsetzung der Datenschutz-Grundverordnung DSGVO in aller Munde. Aber auch über Hackerangriffe und Erpressungsversuche (verschlüsselter Computer wird erst freigegeben, wenn man Lösegeld bezahlt) liest man verstärkt in den Medien, trotzdem die Geschädigten kaum zur Polizei gehen, weil sie sich schämen (private Personen) oder (das trifft auf viele Unternehmen zu) die drohenden Vertrauensverluste bei Konsumenten fürchten. Aber „dank DSGVO" wird schon der bloße **„Datendiebstahl" zu einem existenzbedrohlichen Szenario,** sollten Kundendaten entwendet und dem Betroffenen nachgewiesen werden, dass er seine Hard- und Software bzw. IT-Lösung nicht nach dem aktuellen Stand der Technik ausgerüstet hat.

Unser heutiger Praxistipp weist Sie, werte Leserin, werter Leser, auf eine **überaus nützliche Homepage und deren Newsletter-Service hin**, deren Ziel es ist, auf Betrugsmaschen, Fallen und Fakes im Internet hinzuweisen, um Problembewusstsein zu schaffen und im Idealfall zu helfen, dass man darauf nicht reinfällt.

„Watchlist Internet" ist ein Projekt des **Internet Ombudsmanns** und wird u.a. in Zusammenarbeit mit dem Bundesministerium für Arbeit, Soziales und Konsumentenschutz umgesetzt. Auch besteht eine enge Zusammenarbeit mit der EU-Initiative Saferinternet.at.

Watchlist Internet ist eine **unabhängige Informationsplattform zu Internet-Betrug und betrugsähnlichen Online-Fallen,** die in Österreich auftreten. Sie informiert, welche Betrugsfälle im Internet aktuell passieren und gibt Tipps, wie man sich vor gängigen Betrugsmaschen schützen kann. Opfer von Internet-Betrug erhalten konkrete Anleitungen für weitere Schritte.

Typische **Schwerpunktthemen** der Watchlist Internet sind u.a.: Phishing, Bossing, Abzocke über Smartphone, Abo-Fallen, Fake-Shops, Markenfälschungen, Vorschussbetrug, gefälschte Rechnungen, gefälschte Abmahnungen, Lösegeld-Trojaner.

Wir empfehlen, sich in die Newsletter-Liste einzutragen – hier klicken - denn dann erhält man jeden Freitag einen kurzen Info-Newsletter, der die jeweiligen Gefahren kurz beschreibt und zu weiteren Infos verlinkt.

Typische Beispiele der letzten Wochen aus dem Watchlist-Newsletter:

a) Phishing: Angebliche Sicherheits-App der Erste Bank und Sparkasse ist schädlich!

Betrüger fälschen eine Erste Bank und Sparkasse-Nachricht und versenden diese massenhaft. In der Nachricht wird behauptet, dass das Bankkonto der Empfängerin/des Empfängers eingeschränkt werden musste und zur weiteren Nutzung die Installation einer Sicherheits-App nötig sei. Doch Vorsicht: Es handelt sich bei dem E-Mail um Phishing und bei der App um Schadsoftware. Personen, die den Schritten in der Mail folgen und die Applikation installieren, gewähren den Kriminellen Zugriff auf das eigene Bankkonto.

Mehr Details hier…

b) Warnung vor gefälschter Finanzonline.at-Nachricht

Internet-Nutzerinnen und Nutzer erhalten ein gefälschtes E-Mail des Finanzministeriums. Es hat den Betreff „Ihre Steuerrückzahlung". Darin heißt es, dass eine kürzlich erfolgte Steuerrückzahlung an Empfängerinnen und Empfänger fehlgeschlagen sei. Aus diesem Grund sollen sie auf einer unbekannten Website persönliche Bankdaten bekannt geben. Nutzer übermitteln diese an Kriminelle und werden Opfer eines Datendiebstahls. **Mehr Details** hier…

c) Bossing: Vermeintliche Geschäftsführung drängt zu Geldüberweisung

Verrechnungs- und Buchhaltungsabteilungen in Firmen sowie Kassiere in Vereinen werden gezielt von Betrügern adressiert. Die E-Mails werden im Namen der Geschäftsführung der jeweiligen Firma beziehungsweise des jeweiligen Vereins verschickt. Darin werden die Mitarbeiter dazu aufgefordert hohe Geldbeträge ins Ausland zu überweisen. Wird die Überweisung durchgeführt, ist das Geld verloren.

Mehr Details hier…

d) Datenklau, Scamming: Betrügerische Urlaubsnachricht von Kriminellen

Internet-Nutzerinnen und Nutzer erhalten von ihren Kontakten die Nachricht, dass diese im Ausland seien und Hilfe benötigen, denn sie haben ihre „Tasche verloren samt Reisepass und Kreditkarte". Aus diesem Grund sollen Empfänger/innen Geld mit Western Union ins Ausland überweisen. Es wird Geld für ein „Ticket und die Hotelrechnungen" benötigt. In Wahrheit stammt die Nachricht von Kriminellen. Das Geld ist bei einer Auslandsüberweisung verloren. **Mehr Details** hier**…**

e) Fake-Anwalt: Keine Abmahnung wegen Urheberrechtsverletzung bezahlen

Konsumenten erhalten eine Abmahnung wegen Urheberrechtsverletzung. Darin behaupten Betrüger, dass es auf einer Streaming-Plattform zu einer Rechtsverletzung gekommen sei. Aus diesem Grund sollen Empfänger Geld auf ein ausländisches Konto überweisen. Konsumenten können die Abmahnung ignorieren und müssen keine Zahlung leisten.

Mehr Details hier**…**

Die Watchlist Internet trägt dazu bei, dass **Internetnutzer/innen besser über Online-Betrug Bescheid wissen und kompetenter mit Betrugstricks umgehen lernen**. Dadurch wird das Vertrauen in die eigene Online-Kompetenz sowie auch das Vertrauen in das Internet insgesamt gestärkt.
Und Jede und Jeder kann über ein Meldeformular selbst Internet-Fallen melden und so die Aufklärungsarbeit der Watchlist Internet **aktiv unterstützen**. Das Meldeformular finden Sie hier, oder senden Sie ein E-Mail an: meldung@watchlist-internet.at

Sollten Sie bereits Opfer von Online-Betrug geworden sein, können Sie sich an den **Internet Ombudsmann** (mehr dazu unter https://ombudsmann.at/) und mit einer Betrugsanzeige direkt an die **Polizei** wenden.

Quellen: Mag. Günter Wagner, B2B-Projekte für Versicherungsbranche, Homepage Watchlist Internet und Internet-Ombudsmann