32. Cybercrime Newsletter

29.11.2022

1) Vodafone skrupellos: Kunden-Abzocke unter dem Deckmantel derTelekom

Erneut gerät Vodafone in die Schlagzeilen. Dieses Mal jedoch mit einem besonders miesen Trick. Denn: Man versucht nicht nur Kunden reinzulegen, um ihnen Verträge anzudrehen, sondern macht dies auch noch im Namen der Telekom. Jetzt droht den Verantwortlichen sogar eine Haftstrafe.

Immer wieder beschweren sich Vodafone-Kunden über untergeschobene Verträge. Zurecht, wie Verbraucherzentralen und Co. ein ums andere Mal feststellen. Mitte des vergangenen Jahres sorgte eine äußerst kuriose Geschichte für Aufsehen. So hat eine Vodafone-Mitarbeiterin der Katze einer Kundin einen Vertrag untergejubelt, für den die Kundin zahlen sollte. Doch das ist nur die Spitze des Eisbergs. Kurz zuvor sorgte dieser Fall für Aufsehen. Ein Mitarbeiter des Netzbetreibers missbrauchte dabei sogar die Unterschrift einer Toten, um dem Witwer einen Vertrag unterzuschieben. Und nun kommt es noch dicker. Denn Vodafone verschickte Kundenanschreiben im Namen der Telekom, um an Verträge zu kommen. Das ging so weit, dass der Fall vor das Landgericht Düsseldorf ging. Und den Verantwortlichen von Vodafone droht jetzt sogar Gefängnis.

Mit diesem Telekom-Trick wollte Vodafone Kunden zur Unterschrift bewegen

Stell dir vor, du bist Telekom-Kunde und bekommst ein Schreiben von deinem Netzbetreiber. Im Briefkopf ist das Telekom-T in Magenta und darunter der Slogan „Erleben, was verbindet“. Der Inhalt: Man baue das Telekommunikationsnetz der Zukunft, worauf dein bestehender Telefonanschluss noch nicht abgestimmt sei. Dein bisheriger Vertrag könne aber nicht unverändert übernommen werden. Daraufhin empfiehlt die Telekom in dem Schreiben, die Komplettpakete von Vodafone zu buchen. Doch in Wirklichkeit kommt der Brief gar nicht von der Telekom, sondern von Vodafone.

Der Netzbetreiber behauptet zwar vor Gericht, dass diese Kundenanschreiben von einem Vertriebspartner stammen und dass man keine Kenntnis darüber gehabt habe. Doch das Landgericht Düsseldorf macht hier keinen Unterschied und verurteilt Vodafone (das Urteil liegt der Redaktion von inside digital vor). Schließlich habe der Vertriebspartner die Kundendaten von Vodafone erhalten und wird von dem Netzbetreiber beauftragt, bezahlt und provisioniert.

„Vodafone hat, indem sie ihre Kundendaten außenstehenden Dritten zur Nutzung für den Vertrieb ihrer Produkte zur Verfügung gestellt und Provisionen für vermittelte Vertragsabschlüsse ausgelobt hat, eine von ihr grundsätzlich beherrschbare Gefahrenquelle geschaffen“, lautet die Begründung des Gerichts. Somit hafte Vodafone auch für das sich daraus ergebende Risiko eines missbräuchlichen Verhaltens der eingesetzten Vertriebsleute.

Diese Strafe droht dem Netzbetreiber jetzt

Das Ziel der Vertriebler war klar: Sie wollten Telekom-Kunden einen Vertrag von Vodafone unterschieben. Nun hat das Landgericht diesem Vorgehen einen Riegel vorgeschoben. Vodafone, ob Subunternehmen oder nicht, ist es nicht erlaubt, Kundenanschreiben im Namen der Telekom zu versenden und zu behaupten, der Vertrag des Telekom-Kunden könne nicht unverändert weiterlaufen.

Außerdem darf Vodafone Kunden nicht unter Druck setzen und behaupten, man müsse handeln, da die Telekom den Anschluss ansonsten kündigt. Sollte man dagegen verstoßen, muss der Netzbetreiber mit einer Strafe von 250.000 Euro oder Ordnungshaft von bis zu sechs Monaten für die Verantwortlichen rechnen.
Quelle: https://www.inside-digital.de/news/vodafone-skrupellos-kunden-abzocke-unter-dem-deckmantel-der-telekom

2) Brief, Besuch, Telefonat Rentenversicherung warnt vor Betrugsversuchen

Bei vermeintlichen Kontakten durch die Deutschen Rentenversicherung sollten Rentner besonders vorsichtig sein. Denn derzeit geben sich wieder vermehrt Trickbetrüger als Mitarbeiter der Behörde aus, um Senioren um ihr Geld zu bringen.

Man kennt die Masche aus den Vorjahren. Oder besser, man sollte sie kennen. Getarnt als Mitarbeitende der Rentenversicherung versuchen Betrüger, an persönliche Daten, die Bankverbindung oder gleich an das Geld der Versicherten zu kommen. Dies soll wahlweise in Form eines täuschend echt wirkenden Briefs, eines unangekündigten Besuchs daheim oder eines unerwarteten Telefonats geschehen.

Derzeit kommen vor allem dubiose Anrufe häufig vor, warnt die Deutsche Rentenversicherung (DRV). Im Display des Telefons werde hier sogar die Rufnummer der DRV imitiert. Das soll die Angerufenen in Sicherheit wiegen.

Eine typische Masche der Betrüger am Telefon: Rentner werden aufgefordert, Geld auf ein fremdes Konto zu überweisen. Dabei kann es sich zum Beispiel um Gebühren für die Bearbeitung und Auszahlung von Rentennachzahlungen und "Sonderauslosungen" handeln. Es wird mit Rentenpfändungen, Rentenkürzungen oder anderen Nachteilen gedroht, wenn die Zahlung verweigert wird.

Keinesfalls Geld überweisen

Die Deutsche Rentenversicherung betont, dass ihre Mitarbeitenden oder von ihr beauftragte Personen in keinem Fall telefonisch dazu auffordern, Geld ins In- oder gar Ausland zu überweisen. Wer einen entsprechenden Anruf erhalten hat, kann sich gern an das kostenfreie Servicetelefon der Deutschen Rentenversicherung unter 0800 1000 4800 wenden.

Hier kann die Broschüre "Vorsicht Trickbetrüger" heruntergeladen werden. Darin stellt die Deutsche Rentenversicherung ein paar Betrugsmaschen vor und erklärt, wie man sich am besten schützen kann. Die Broschüre wendet sich nicht nur an Rentnerinnen und Rentner, sondern ausdrücklich auch an Angehörige und Nachbarn älterer Menschen sowie Mitarbeiter von Pflegediensten, denn in Zweifelsfällen können sie wertvolle Ansprechpartner sein, um Betrug zu verhindern. Denn leichtes Spiel hat ein Täter, wenn er mit seinem Opfer allein ist. Deshalb sollten Kontaktierte im Zweifel immer eine Vertrauensperson hinzuziehen – ganz besonders, wenn diese sich unter Druck gesetzt fühlen.
Quelle: https://www.n-tv.de/ratgeber/Brief-Besuch-Telefonat-Rentenversicherung-warnt-vor-Betrugsmaschen-bei-Senioren-article23717773.html

3) Enkeltrick neu erfunden – Dringende Warnung vor Fake-Mails von den Behörden zur Energiepauschale

Die 300 Euro der Energiepauschale kommt für Rentner automatisch. Wer am Telefon oder per Mail Kontodaten haben will, ist ein Betrüger.

Dortmund – Der Enkeltrick ist keine neue Betrugsmasche und trotzdem wird er bei nichtsahnenden Rentnern noch immer erfolgreich angewendet. Die Energiepauschale bietet nun ganz neue Möglichkeiten für die Betrüger, denn aktuell warten viele Menschen auch in Hamburg noch auf die Ausgleichszahlung der Regierung für die gestiegenen Energiekosten. Deshalb bekommen jetzt viele Betroffene E-Mails oder Anrufe, in denen behauptet wird, sie müssten noch einmal ihre Kontodaten angeben, um die Energiepauschale zu bekommen. Solche Nachrichten sind Betrug, berichtet 24hamburg.de!

Fake-Mails von den Behörden: Betrug mit Energiepauschale für Rentner

„Die Regierung hat beschlossen, dass Sie eine Erstattung von 278,35 Euro erhalten werden. Hier klicken, um die Zahlung zu erhalten.“ Wer eine E-Mail oder eine SMS mit diesem oder einem ähnlichen Text erhält, sollte eines tun: Löschen und blockieren!

Die Nachrichten, die gerade viele Verbraucher bekommen, sind eine betrügerische Masche, mit denen man sich entweder einen Virus auf den eigenen Computer zieht oder Betrügern Zugang zum eigenen Bankkonto verschafft. Der vermeintliche Absender ist zum Beispiel das Bundesamt für Finanzen oder die eigene Bank. Die Verbraucherzentrale Saarland warnt davor, nicht auf solche Nachrichten einzugehen. Übrigens rufen derzeit mehrere Kampagnen zur Spende der Energiepauschale auf – auch Rentner profitieren.

Denn auch wenn die Mails noch so echt aussehen, sie sind ein Fake - wie auch zuletzt die Fake-Anrufe von Europol. Für die Energiepauschale braucht nämlich niemand irgendwo seine Daten anzugeben. Die 300 Euro von der Pauschale kommen automatisch mit dem Gehalt oder der Rente, ohne dass der Verbraucher extra aktiv werden muss. Auch Studenten erhalten bald eine Energiepauschale.

Betrug am Telefon: Neue Version des Enkeltricks für Energiepauschale

Laut der Deutschen Rentenversicherung kommt es aktuell auch immer häufiger vor, dass Rentner unter dem gleichen Vorwand angerufen werden. Die Betrüger am anderen Ende der Leitung behaupten dann, für die Überweisung der Energiepauschale noch einmal die Kontodaten zu benötigen oder abgleichen zu müssen. Es ist das gleiche Prinzip wie beim Enkeltrick oder „Hallo Mama“-Nachrichten bei What‘s App.

Auch hier gilt: Nicht drauf reinfallen! Wer Rente bezieht, bekommt die 300 Euro der Pauschale von der Rentenversicherung automatisch, denn diese hat die Kontodaten der Rentenbezieher bereits vorliegen. Es gibt also keinen Grund, sie noch einmal am Telefon durchzugeben. Diese Anrufe kommen von Betrügern, die ihre Opfer manchmal um Millionen erleichtern.

Wer zu spät merkt, dass sich am anderen Ende der Leitung ein Betrüger verbirgt, und bereits Daten herausgegeben hat, sollte dann schleunigst auflegen und die Polizei sowie die eigene Bank informieren. Unrechtmäßig eingezogene Beträge können meist von den Geldinstituten zurückgeholt werden.

Energiepauschale für Rentner: 300 Euro kommen im Dezember 2022

Arbeitnehmer und Selbstständige haben die 300 Euro der Energiepauschale bereits im September bekommen. Entweder kam das Geld mit dem Gehalt durch den Arbeitgeber beim Endverbraucher an, oder es kam Selbstständigen und Freiberuflern durch eine Ermäßigung in der Einkommenssteuervorauszahlung zugute. Bisher gingen Rentner leer aus, weil sie nicht erwerbstätig sind.

Das dritte Entlastungspaket des Bundes hat das nun geändert. Auch Rentner sollen jetzt von der Energiepauschale profitieren, die über die Deutsche Rentenversicherung ausgezahlt wird. Der Zeitpunkt der Auszahlung für die Energiepauschale für Rentner ist der 1. Dezember, spätestens aber der 15. Dezember. Bezieher von Rentengeld müssen also nichts weiter tun, als auf den Eingang der einmaligen Zahlung zu warten - und manche Rentner können die Energiepauschale sogar doppelt kassieren. Die einzige Ausnahme bilden Rentner, die im Dezember 2022 auch zum ersten Mal eine Rentenzahlung erhalten werden. Bei ihnen kann sich die Auszahlung aus technischen Gründen noch etwas hinziehen, erfolgt aber ebenfalls automatisch im neuen Jahr.

Der einzige Haken: Auch Rentner müssen die 300 Euro der Energiepauschale versteuern und bei der Einkommenssteuer berücksichtigen. Je niedriger die Steuer, desto mehr bleibt von der Pauschale übrig. Wer unter dem Freibetrag bleibt, profitiert sogar von der ganzen Summe.
Quelle: https://www.ruhr24.de/service/auszahlung-energiepauschale-24h-betrug-betrugsmasche-verbraucher-termin-2022-rentner-91937390.html

4) PayPal-Kunden müssen um ihr Geld fürchten – So knacken Kriminelle Konten

Das Gefährliche an Phishing ist, dass man nie voraussagen kann, in welche Verkleidung der schädliche Link verpackt wird. Mal ist es eine DHL-Mail, mal eine angebliche Konto-Sperrung, mal eine Bank. Wir verraten, welche Phishing-Mails in der 47. Jahreswoche verbreitet sind.

Die Verbraucherzentrale NRW listet im Rahmen ihres Phishing-Radars kontinuierlich die neuesten Phishing-Mails auf. Selbstverständlich ist die Liste nicht erschöpfend; auch andere Mails sind im Umlauf. Sie zeigt allerdings, bei welchen E-Mails man als Nutzer derzeit auf jeden Fall ein Auge offen halten sollte. In der laufenden Woche gehören dazu die folgenden Unternehmen und Organisationen:

- PayPal
- Sparkasse
- Postbank
- FedEx

Aktuelle Phishing-Lage – PayPal, Banken und Paketdienste

PayPal

Es bedarf nur eines einzigen Fehlers und schon haben Dritte dein PayPal-Konto geknackt und können sich nach Herzenslust bedienen. Dieser „Fehler“ lässt sich dabei üblicherweise auf eine Phishing-Mail zurückführen, welche bereits seit vergangener Woche im Namen des beliebten Online-Bezahldienstes verschickt wird. Die Empfänger werden zunächst damit konfrontiert, dass ihr PayPal-Konto „vorübergehend eingeschränkt“ ist. Der Grund: Eine neue

Zahlungsrichtlinie der Europäischen Kommission soll alle Banken und Zahlungsdienstleister angeblich dazu verpflichten, einen Datenabgleich ihrer Kunden einzufordern. Da dies bislang nicht erfolgt ist, wurde das Konto gesperrt. Nun muss besagter Datenabgleich über eine in der E-Mail hinterlegte Verlinkung angestoßen werden, um das PayPal-Konto wieder in vollem Umfang nutzen zu können. Das geht zumindest aus der E-Mail hervor.

In Wahrheit führt die Verlinkung allerdings zu einer gefälschten PayPal-Website. Sämtliche hier eingetragenen Nutzer- und Anmeldedaten landen daher bei den Cyberkriminellen. Und selbst die sogenannte Zwei-Faktor-Authentifizierung (2FA) schützt den Zugang nur, solange die Nutzer ihren SMS-Code nicht ebenfalls an die Kriminellen übermitteln. Daher empfiehlt es sich, bei zweifelhaften Nachrichten ohne direkte Kundenansprache oder mit zahlreichen Rechtschreibfehlern von einem Klick abzusehen und diese stattdessen in den Spam-Ordner zu befördern. Schließlich bedarf es lediglich einer schnellen Anmeldung bei PayPal, um die Echtheit der E-Mail zu überprüfen.

Postbank

Postbank-Kunden werden in einer E-Mail inhaltlich wieder einmal mit der sogenannten BestSign App konfrontiert. Laut den Absendern sei ein Abgleich der Mobilfunknummer notwendig, um diese weiterhin in vollem Umfang nutzen zu können. Dies sei zwingend erforderlich, um die Sicherheit im Mobilfunknetz zu gewährleisten – was auch immer das in diesem Zusammenhang zu bedeuten mag. Die Phishing-Mail selbst wirkt optisch ansprechend und überzeugt auch grammatikalisch. Allerdings fehlt eine direkte Kundenansprache. Zudem offenbart ein Klick auf den Absender, dass die E-Mail nicht vonseiten der Postbank verschickt wurde. Sollten dennoch Zweifel an der Echtheit der Nachricht bestehen, empfiehlt es sich, der Anweisung der Cyberkriminellen Folge zu leisten, und Kontakt mit dem Kundenservice aufzunehmen. Die dazu erforderlichen Kontaktinformationen sollten Betroffene jedoch unbedingt eigenständig heraussuchen.

Sparkasse

Kunden der Sparkasse stehen derzeit unter Beschuss und müssen sich auf gleich mehrere unterschiedliche Phishing-Mail einstellen. Die erste thematisiert eine aktuelle und EU-weite Änderung an der „Payment Service Directive 2“. Es folgt eine abenteuerliche Erklärung, mit Fokus auf der Einführung eines Fingerabdruck-Profils, welcher unter Zuhilfenahme künstlichen Intelligenz angefertigt wird. Doch bevor dies geschieht, sei eine Umstellung mit abschließender Verifizierung des Kontos notwendig – „um Ihren Fingerprint für die künstliche Intelligenz zu trainieren“. Interessant ist, dass die E-Mail diesmal sogar über eine direkte Kundenansprache zu verfügen scheint. Doch auch das ist kein Garant für die Echtheit einer E-Mail, denn die dafür benötigten Informationen können aus einem früheren Datenleck stammen. Wenn du wissen möchtest, ob ein mit deiner E-Mail verknüpftes Konto schon einmal gehackt wurde, kannst du kostenfrei eine automatische Benachrichtigung einrichten.

Die zweite E-Mail lässt sich derweil so leicht als Phishing-Mail enttarnen, dass man den Eindruck bekommen könnte, diese werde nur verschickt, um die zuvor erwähnte Nachricht glaubwürdiger dastehen zu lassen. Sie beginnt beispielsweise mit der folgenden Erläuterung: „Der Sicherheit wegen kommt es immer wieder zu verbessertenGesetzesauflagen, um Ihnenhöchstmögliche Sicherheit zu regenerieren.“

FedEx

Was vergangene Woche Hermes war, ist nun FedEx. Inhaltlich geht es darum, dass ein Paket nicht zugestellt werden konnte. Nun benötige man „eine Adressbestätigung, um den Versand

des Pakets zu bestätigen.“ Es folgt eine Verlinkung, die abermals nicht angeklickt werden sollte. Direkte Kundenansprache? Fehlanzeige. Ein klarer Fall für den Spam-Ordner. Zumal selbst die Optik nicht der des US-amerikanischen Logistikunternehmens entspricht, sondern kurzerhand von Hermes übernommen wurde. Dafür haben die Betrüger ein Bild von einem FedEx-Fahrzeug hinzugefügt.

Phishing 2022 – Bisherige Fälle

Die Liste an Phishing-Versuchen in Deutschland wird immer länger. Klar zu erkennen ist, dass es vorwiegend große Unternehmen betrifft. Sie haben viele Kunden und damit viele potenzielle Opfer von Phishing. Diese Liste zeigt, welche Unternehmen im Jahr 2022 schon von Phishing-Betrügern genutzt wurden, um deine Daten oder dein Geld zu stehlen:

- 1&1
- Advanzia Bank
- Amazon
- Apple
- BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht)
- Barclays
- Bitcoin-Erpressung
- Bundesregierung
- Commerzbank
- Deutsche Bank
- Deutsche Kreditbank (DKB)
- DHL
- Disney+
- DPD
- Hermes
- IHK
- Ionos
- ING
- Instagram
- Landesbank Berlin (LBB)
- Netflix
- PayPal
- Postbank
- SMS (Voicemail)
- Sparkasse
- Targobank
- Telekom
- Volks- und Raiffeisenbanken
- WEB.DE
- WhatsApp
- Zollamt

Was ist Phishing eigentlich?

Wenn man an Cyberkriminelle denkt, kommen einem automatisch Hollywood-Bilder von Unbekannten in Kapuzenpullis in den Sinn, die in einem Keller vor fünf Bildschirmen sitzen und ihren Blick auf das Pentagon richten. Die Wahrheit sieht allerdings oftmals ganz anders aus. Denn man braucht weder fünf Bildschirme noch große Kenntnisse über

Sicherheitssoftware, um an das Geld von Internetnutzern zu gelangen. Sogar ein Kapuzenpulli ist dafür nicht zwingend erforderlich. Viele Anwender verraten ihre Zugangsdaten nämlich freiwillig, wenn man sie darum bittet.

Alles, was dazu benötigt wird, ist eine E-Mail im beispielsweise Amazon-Look, die Empfänger über ungewöhnliche Kontoaktivitäten oder eine AGB-Änderung unterrichtet. Anschließend wird das Opfer dazu aufgefordert, eine Autorisierung durchzuführen, indem er einen Link anklickt und sich in seinem Account anmeldet. Nur führt der Link nicht zur Amazon-Website, sondern zu einer Kopie. Die hier eingetragenen Login-Daten landen direkt bei den Cyberkriminellen. Mittlerweile steckt hinter Phishing eine regelrechte Industrie.

Weitere Betrugsmaschen & Schutzmechanismen:

- eBay Kleinanzeigen und Co.: Mit diesen Betrugsmaschen zockt man dich ab
- WhatsApp Abzocke: Das sind die hinterlistigen Maschen der Betrüger
- Privatsphäre durch Zukleben der Webcam? So löst du das Problem eleganter

So erkennst du Phishing-Mails

Sobald die Betrüger deine Nutzerdaten erbeutet haben, können sie diese beispielsweise zum Identitätsdiebstahl verwenden. Sollten die Anmeldedaten zu einem mit dem **Bankkonto** verknüpften Dienst gehören, könnte auch dein Portemonnaie darunter leiden. Darum solltest du auf E-Mails im Allgemeinen und auf Nachrichten der oben genannten Anbieter im Besonderen achten. Weist die E-Mail Rechtschreibfehler auf? Wie sieht es mit direkter Kundenansprache aus? Handelt es sich bei dem Absender respektive bei der E-Mail-Adresse des Absenders im Kopf der E-Mail tatsächlich um PayPal? Gehört die verlinkte Webseite dem Online-Bezahldienst, oder ist die URL eher kryptisch? Alle diese Fragen können eine Phishing-Mail enttarnen.

Eine weitere, gute Selbstschutz-Maßnahme stellt die Zwei-Faktor-Authentifizierung (2FA) dar. Dabei handelt es sich um einen doppelten Anmeldeschutz, bei dem neben den Anmeldedaten eine zweite Anmeldeschranke eingerichtet wird – etwa in Form eines Codes, der auf eine zuvor hinterlegte Telefonnummer zugestellt wird. Diesen können Cyberkriminelle in der Regel nicht so einfach ergattern. Obwohl auch diese Schutzlinie nicht unüberwindbar ist. Weitere Informationen zu dem Thema erhältst du in unserem Phishing-Ratgeber

Quelle: https://www.inside-digital.de/news/phishing-woche-aktuelle-faelle-kw47-paypal-konten-geknackt

5) Ransomware: Was machen Erpressungstrojaner?

Ransomware – auch "Erpressungstrojaner" genannt: Was soll man sich darunter vorstellen? Lassen Sie sich eins gesagt sein: Der deutsche Name ist Programm! Die wichtigsten Infos und Verhaltenstipps finden Sie in diesem Artikel.

Nichts ist, wie es scheint. Was beim Trojanischen Pferd einst der Fall war, trifft auch beim Erpressungstrojaner zu: Denn die Gefahr ist von außen nicht sichtbar, sie schlummert gut getarnt im Innern.

Was sind Erpressungstrojaner?

"Ransom" (auf Deutsch: "Lösegeld") – kombiniert mit dem Ende des Wortes "Software" − ergibt den Ausdruck **Ransomware**. Das passt auch: Das Ziel von Erpressungstrojanern ist nämlich die Erpressung von **Lösegeld**. Das Druckmittel: Ihr mittels Schadsoftware gesperrter Rechner oder ein bestimmtes Laufwerk.

Erpressungstrojaner – so läuft das Ganze ab

Hacker gehen bei Trojaner-Angriffen wie folgt vor:

1. Sie **schleusen gut getarnte Malware** auf Ihren PC oder Ihr Handy. Wie? Nun, es gibt verschiedene Möglichkeiten:

- Durch manipulierte Anhänge in Spam-Mails (z. B. unter dem Deckmantel von angeblichen Rechnungen oder Mahnungen)
- über Phishing-Links,
- oder über infizierte Werbeflächen und gefälschte Webseiten. Mit einem versehentlichen Klick darauf aktivieren Sie die heimliche Installation der Schadsoftware.

Wie echte Viren haben Erpressungstrojaner manchmal eine gewisse **Inkubationszeit**. Dadurch kann es sein, dass Sie sie erst gar nicht bemerken. Und genau das spielt den Hackern in die Karten: Sie sollen sich nicht daran erinnern können, wann oder wodurch Sie sich den Schädling eingefangen haben – so ist der **Ursprungsort der Malware kaum mehr feststellbar**.

Aber: Erkennen Sie die Malware bereits vor der Lösegeldforderung, haben Sie höhere Chancen, diese direkt wieder entfernen zu können. Hier finden Sie Anzeichen, dass Sie Schadsoftware auf Ihrem Rechner haben.

2. Wenn Sie auf einen verseuchten Anhang, Link etc. geklickt haben, zeigt sich schnell, welche Art von Ransomware Sie befallen hat: Entweder **sperren Screenlocker Ihren gesamten Bildschirm** oder es werden spezifischen **Daten** (Text-Dateien, Fotos, Ordner) **verschlüsselt**.

Das Resultat bleibt jedoch das Gleiche: **Sie können nicht mehr auf Ihr virtuelles Hab und Gut zugreifen!**

3. Jetzt erhalten Sie eine Meldung: Angeblich bekämen Sie nur mit Lösegeld Ihre Daten wieder. Doch es kann noch übler kommen: Manche Ransomware-Varianten drohen auch damit, Ihre Daten zu veröffentlichen, wenn Sie nicht zahlen!

Sollte ich das Lösegeld zahlen?

Eine ausdrückliche Warnung davor und ein **ganz klares Nein**! Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät davon ab – denn nur in den seltensten Fällen halten die Kriminellen auch ihr Versprechen. In der Regel verlieren Sie so also nicht nur Ihre Daten, sondern auch das Geld.

Und Sie schneiden sich damit auch noch ins eigene Fleisch: Dadurch steigt nämlich die Wahrscheinlichkeit, dass Sie **erneut Ziel eines Ransomware-Angriffs** werden, da Sie bereits Zahlungsbereitschaft gezeigt haben.

Wie verhalte ich mich richtig?

1. Eventuell handelt es sich gar nicht um einen echten Trojaner – tatsächlich wird dies in manchen Fällen nur vorgespielt. Also: **Prüfen Sie zuerst**, ob die Bedrohung echt ist.
2. Bei Ihnen ist wirklich ein Trojanisches Pferd eingedrungen? Dann sollten Sie umgehend **jegliche Verbindungen** (virtuell sowie physisch) **zu anderen Geräten entfernen** – z. B. zu externen Festplatten oder Speichermedien. Sonst könnte sich die Ransomware sogar noch innerhalb des Netzwerkes verbreiten.
3. Führen Sie einen Virenscan durch und löschen Sie die Malware.

4. Wenn bei Ihnen bereits Daten verschlüsselt wurden, existiert mit Glück vielleicht schon eine Entschlüsselungssoftware für den Trojaner. Andernfalls sollten Sie am besten Fachleute zu Rate ziehen – denn hier könnte es nicht nur kompliziert, sondern auch riskant werden.

Im Worst Case…

…nützt manchmal alles nichts. Schlimmstenfalls müssen Sie Ihr System auf den Werkszustand – oder, wenn Sie regelmäßig Systembackups durchführen, auf den letzten Zustand – zurücksetzen. Dabei sollte Ihnen bewusst sein, dass dadurch Ihre Daten auf dem Gerät verloren gehen – insofern Sie keine zusätzliche Datensicherung durchgeführt haben.

Präventive Maßnahmen

Diese Katastrophe lässt sich jedoch schon mit einem geringen Aufwand vermeiden:

- Öffnen Sie nicht unbedacht E-Mail-Anhänge oder Links. Seien Sie generell auf der Hut vor Spam und Phishing-Attacken. Diese treten vermehrt in Aktionswochen wie der Black Week oder zu bestimmten Anlässen wie der Weihnachtszeit auf.
- Führen Sie regelmäßige Sicherheitsupdates Ihres Betriebssystems und Ihrer Programme durch.
- Installieren Sie eine Anti-Viren-Software und nutzen Sie eine Firewall.
- Erstellen Sie regelmäßig Backups Ihrer Dateien – dazu eignet sich sehr gut die Cloud.

Quelle: https://navigator.gmx.net/blog?sid=054538a662f1ab714dcb21dc4e341d6015114a3aeaaa605f2731ed801c1105948144f264aa080997f858495932a97223

6) Gewaltiger WhatsApp-Skandal: Darauf musst du im Messenger jetzt aufpassen

Nun ist es passiert: Hacker haben bei WhatsApp offenbar die unglaubliche Summe von einer halben Milliarde Kontodaten geklaut. Allein in Deutschland sind 6 Millionen WhatsApp-Nutzer betroffen. Und alle, die den Messenger nutzten, sollten sich jetzt in Acht nehmen.

WhatsApp und Facebook geraten immer wieder ins Visier von Datenschützern. Zwar argumentiert der Mutterkonzern Meta immer mit Ende-zu-Ende-Verschlüsselung, doch schon länger ist klar, dass das Unternehmen Daten zu Gruppennamen, deren Mitgliedern, Profilnamen, Fotos und auch IP-Adressen auswerte. Und nun sind sensible Daten in die Finger von Hackern geraten – schon wieder. Dieses Mal sind nicht Facebook-Nutzer die Leidtragenden, sondern 500 Millionen WhatsApp-Nutzer. Und diese müssen jetzt höllisch aufpassen.

WhatsApp und der größte Datenskandal aller Zeiten

Vor wenigen Tagen, am 16. November, macht ein Nutzer eines bekannten Hacker-Forums in ebenjenem bekannt, dass er eine Datenbank aus dem Jahr 2022 mit 487 Millionen Handynummern von WhatsApp-Nutzern verkauft. Da WhatsApp weltweit etwa zwei Milliarden aktive Nutzer hat, sind ein Viertel aller Menschen betroffen, die den Messenger auf dem Handy installiert haben. Wie Cybernews berichtet, sollen allein in Deutschland sechs Millionen Handynummern zum Verkauf stehen.

Das ist in dem ganzen WhatsApp-Skandal auch die einzig gute Nachricht. Denn offenbar soll

es nur um Handynummern gehen. Sie stehen angeblich nicht in Verbindung mit Namen, Profilbildern oder anderen sensiblen Daten. Es gibt aber auch schlechte Nachrichten. Denn: Noch lässt sich nicht sagen, ob die eigene Handynummer zu dem Verkaufspaket gehört. Zwar gibt es Dienste wie „Have I Been Pwned?„, die anhand von Namen oder Handynummern feststellen könne, ob man gehackt wurde. Doch diese haben den Datensatz wohl noch nicht integriert.

Das musst du jetzt tun

Durchgesickerte Handynummern könnten diejenige, die sie kaufen, für Marketingzwecke, Phishing, Identitätsdiebstahl und Betrug benutzen. Solltest du bei WhatsApp demnächst Nachrichten von unbekannten Nutzern und Telefonnummern bekommen, solltest du unter keinen Umständen auf Links in den Nachrichten tippen. Auch auf den Download von Fotos, Videos und anderen Dateien solltest du verzichten. Am besten, du reagierst auf Nachrichten eines Unbekannten bei WhatsApp gar nicht und blockierst den Nutzer.

Sollte er sich als deine Mutter, dein Vater oder ein anderes Familienmitglied ausgeben, das in Not ist, prüfe das vorher. Ruf das vermeintliche Familienmitglied an und versichere dich, ob es wirklich einen Notfall gibt. Wie solch ein Trick funktioniert, zeigen wir dir in diesem Beitrag. Sei wachsam und helfe älteren Verwandten ohne technisches Know-how, die WhatsApp nutzen, um etwa mit ihren Enkeln zu kommunizieren. Hacker und Verbrecher kommen immer wieder auf neue Ideen, die sich manchmal nur schwer durchschauen lassen.

Tipp: Erschreckend: Das alles weiß WhatsApp über dich

Quelle: https://www.inside-digital.de/news/gewaltiger-whatsapp-skandal-darauf-musst-du-im-messenger-jetzt-aufpassen

7) Geheimcodes für die FritzBox: Wer diese kennt, kann mehr mit dem Router machen

Fritzboxen sind für ihre Funktionsvielfalt bekannt. Was viele Nutzer nicht wissen: Per Tastencodes auf angeschlossenen Telefonen können Sie den WLAN-Router fernsteuern. Wir zeigen Ihnen die praktischsten Codes.

Es gibt verschiedene Möglichkeiten, um die Fritzbox zu bedienen. Erste Anlaufstelle für größere Änderungen an den Einstellungen ist die Browser-Oberfläche über http://fritz.box. Alternativ können Sie in kleinerem Umfang auch die Apps von AVM verwenden, etwa die MyFritzApp oder zu Drittanbieter-Apps wie CheckMyBox oder BoxToGo greifen.

Doch das war es noch lange nicht. Besitzt Ihre Fritzbox eine eingebaute Telefonbasis, können Sie den WLAN-Router auch per Telefon fernsteuern. So einfach wie mit einer App funktioniert das aber nicht, denn Sie müssen kryptische Codes eintippen. Wir zeigen, was damit möglich ist.

Tastencodes steuern die Fritzbox

Sie brauchen nicht viel, um Ihre Fritzbox über das Telefon zu steuern. Ein angeschlossenes Telefon reicht. Dabei ist es egal, ob es sich um ein Schnurlostelefon handelt oder das Telefon per Kabel direkt an der Fritzbox hängt. Bringen Telefone eine eigene Basis mit, muss eingestellt sein, dass es Sonderzeichen wie * und # wählen kann.

Leider klappt die Steuerung der Fritzbox nicht über ein Smartphone mit der FritzApp Fon. Einzige Ausnahme sind interne Anrufe. Mit IP-Telefonen funktionieren nur wenige

Tastencodes, etwa Rufnummer einmalig unterdrücken oder Rufumleitung an-/ausschalten.

Zur Eingabe der Codes tippen Sie dann statt einer Telefonnummer eine der unten angegebenen Zeichenfolgen ein. In der Regel beginnen sie mit # oder *. Achten Sie darauf, wirklich exakt alle Zeichen einzutippen und drücken Sie danach die Hörertaste, um den Code an die Fritzbox zu schicken. Bei Telefonen ohne Hörertaste müssen Sie erst den Hörer abnehmen und danach den Code eintippen.

Beispiele für Tastencodes:

- **#96*0*:** WLAN ausschalten
- **#96*1*:** WLAN einschalten
- **#881**:** Weckruf einschalten (muss unter "Telefonie/Weckruf" eingerichtet sein)
- **#881#:** Weckruf ausschalten
- **#990*15901590*:** Neustart der Fritzbox
- **#991*15901590*:** Fritzbox auf Werkseinstellungen setzen (Achtung, nur als letztes Mittel verwenden, setzt alle Fritzbox-Einstellungen zurück)

Telefonfunktionen direkt ändern

Viele der Codes, die Sie am Telefon zur Fritzbox-Konfiguration verwenden können, betreffen Telefoniefunktionen. So können Sie zum Beispiel die Rufumleitung festlegen, den Anrufbeantworter abrufen oder Ihre Rufnummer unterdrücken. Wenn Sie noch mehr Tastencodes ausprobieren wollen, empfiehlt sich ein Blick ins Fritzbox-Handbuch.

- ***21*ZRN*Rufnummer#:** Rufumleitung zu Zielrufnummer (ZRN) aktivieren
- ***21**Rufnummer#:** Sofortige Rufumleitung ausschalten
- ****600:** Anrufbeantworter 1 anrufen
- ****601:** Anrufbeantworter 2 anrufen
- ****9:** internen Rundruf starten
- ***31#:** Rufnummer einmalig unterdrücken

Quelle: https://www.chip.de/news/Geheimcodes-fuer-die-FritzBox-Wer-diese-kennt-kann-mehr-mit-dem-Router-machen_184525445.html

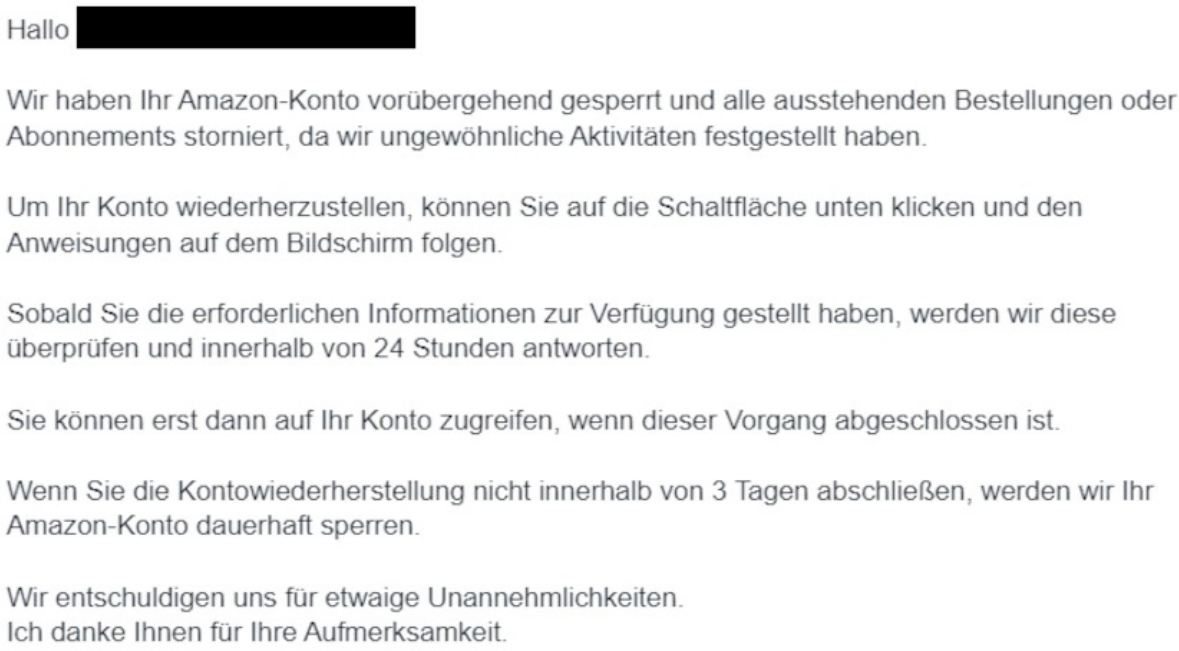
8) Betrugsmasche bei Amazon: Verbraucherzentrale warnt vor neuer Abzocke

Gefahr für Amazon-Nutzer: Die Verbraucherzentrale warnt aktuell vor einer neuen Masche, mit der Kriminelle an Ihre Daten wollen. Wir haben alle Details.

Amazon-Nutzer sind mal wieder ins Visier von Betrügern geraten. Wie die Verbraucherzentrale berichtet, häufen sich seit einigen Tagen Meldungen über neue Phishing-Mails. Darin wird behauptet, dass das Konto aufgrund von "ungewöhnlichen Aktivitäten" vorübergehend gesperrt worden sei.

Um es wiederherzustellen, müsse man auf einen beigefügten Link klicken und in Folge den Anweisungen auf dem Screen folgen und eine Reihe von sensiblen Daten angeben. Kommt man dem nicht innerhalb von drei Tagen nach, wird das Konto dauerhaft gesperrt. Nach der Durchführung werden die Daten angeblich geprüft und Nutzer erhalten innerhalb von 24 Stunden eine Antwort.

Amazon-Betrugsmasche: So verhalten Sie sich richtig


Hallo [redacted]

Wir haben Ihr Amazon-Konto vorübergehend gesperrt und alle ausstehenden Bestellungen oder Abonnements storniert, da wir ungewöhnliche Aktivitäten festgestellt haben.

Um Ihr Konto wiederherzustellen, können Sie auf die Schaltfläche unten klicken und den Anweisungen auf dem Bildschirm folgen.

Sobald Sie die erforderlichen Informationen zur Verfügung gestellt haben, werden wir diese überprüfen und innerhalb von 24 Stunden antworten.

Sie können erst dann auf Ihr Konto zugreifen, wenn dieser Vorgang abgeschlossen ist.

Wenn Sie die Kontowiederherstellung nicht innerhalb von 3 Tagen abschließen, werden wir Ihr Amazon-Konto dauerhaft sperren.

Wir entschuldigen uns für etwaige Unannehmlichkeiten.
Ich danke Ihnen für Ihre Aufmerksamkeit.

Amazon-Kunden müssen aufpassen: Mit diesen Phishing-Mails wollen die Angreifer an Ihre Daten kommen. Verbraucherzentrale

Haben Sie eine derartige Mail erhalten, sollten Sie sich auch von der sehr kurzen Frist nicht verunsichern lassen. Es handelt sich wie so oft lediglich um einen Versuch von Betrügern, Druck auf Sie aufzubauen, um an Ihre Daten zu gelangen.

Stattdessen raten wir Ihnen, die Nachricht umgehend unbeantwortet in Ihren Spam-Ordner zu verschieben und keinesfalls über den beigefügten Link Ihre Daten anzugeben. So erkennt Ihr Mailing-Client künftig besser, ob es sich bei Mails um Spam beziehungsweise Phishing-Versuche handelt.

Quelle: https://www.chip.de/news/Verbraucherzentrale-warnt-vor-gefaehrlicher-Amazon-Betrugsmasche_184519632.html

9) "Sicheres Bezahlen" – Polizei warnt vor Betrug über Ebay-Kleinanzeigen

Betrüger wollen über Ebay-Kleinanzeigen an die Kreditkartendaten von Nutzern kommen. Die Polizei warnt vor dieser neuen Betrugsmasche.

Die Funktion "Sicheres Bezahlen" beim Onlineportal Ebay-Kleinanzeigen wird von Betrügern ausgenutzt, warnt das Landeskriminalamt Niedersachsen auf seiner Seite. Kriminelle versuchten über die Option an die Kreditkartendaten von Nutzer zu gelangen.

So gehen die Betrüger laut LKA Niedersachsen vor:

Verkäufer erhielten eine Nachricht von einem potenziellen Interessenten mit dem Hinweis, dass der Artikel mit einer Debitkarte bezahlt worden sei. Und weiter: "Sie werden in Kürze eine Benachrichtigung von Ebay über Ihre Bestellung erhalten".

Zuvor soll der angebliche Käufer die Mobilfunknummer des Verkäufers erfragt haben. Darum

erhalte der Verkäufer im Anschluss an die erste Nachricht oder "nahezu zeitgleich" eine Meldung per SMS, dass die Bezahlung angenommen werden müsse.

Link in SMS führt zu einer Seite der Betrüger

"Diese SMS soll durch den automatisiert klingenden Text den Eindruck erwecken, von Ebay-Kleinanzeigen zu stammen", schreibt das LKA. In der Kurznachricht befinde sich ein Link zu einer Phishing-Seite, in der Kreditkartendaten des Empfängers abgefragt werden.

Danach werde vermutlich eine Zahlung ausgelöst, um den Käufer in die Irre zu führen, heißt es weiter. In einzelnen Fällen schafften es die Täter dann auch noch, "Probleme bei der Zahlung vorzugaukeln, um eine erneute Zahlung bestätigen zu lassen".

Bank sofort informieren

Wenn ein Empfänger auf die Betrugsmasche hereingefallen sein sollte, müsse er sofort seine Bank informieren. "Lassen Sie die Zahlungen sperren", rät das LKA. Vorsorglich sollte auch die betroffene Kreditkarte gesperrt werden.

Auch die Zugangsdaten für den Account von Ebay-Kleinanzeigen sollte der Nutzer ändern. Zudem bittet das LKA Niedersachsen, dass Betroffene eine Anzeige bei einer Polizeidienststelle oder online stellten.

Quelle: https://www.t-online.de/digital/zukunft/id_100084016/betrug-bei-ebay-kleinanzeigen-polizei-warnt-vor-neuer-kreditkarten-masche.html

10) WhatsApp greift durch: Das ist jetzt im Messenger verboten

WhatsApp will den Schutz eurer Privatsphäre erhöhen und schließt ein Schlupfloch beim Versand von Bildern und Videos. Folgendes ist ab sofort nicht mehr im Messenger möglich.

Der Messenger WhatsApp verstärkt den Schutz eurer Privatsphäre und schließt ein Schlupfloch in der Funktion "Medien zur Einmalansicht versenden". Bislang war es möglich diese über die Screenshot-Funktion eures Handys abzufotografieren und sie so unbemerkt doch zu speichern. Das ändert sich nun.

Den Versuch eines Screenshots quittiert der Messenger jetzt in diesem Fall mit einem Hinweis, dass der Screenshot aufgrund einer Sicherheitsrichtlinie nicht aufgenommen werden kann. Auch die Verwendung eines Screenrecorders blockt die App. Das Screenshot-Verbot gilt aber nur für den genannten Part der App. Von Chatliste und Co. könnt ihr weiter Bildschirmfotos anfertigen, ohne dass eure Kontakte darüber benachrichtigt werden.

Einschränkungen bei WhatsApp Web

Die Änderung hat aber auch Auswirkungen auf WhatsApp Web. Hier ist das Versenden von Medien zur Einmalansicht sowie das Öffnen empfangener Dateien nicht mehr möglich. Warum erklären wir euch im verlinkten Artikel.

Es sei jedoch darauf hingewiesen, dass auch nach der Änderung der Empfänger des Inhalts weiterhin die Möglichkeit hat von diesem Aufnahmen anzufertigen - etwa, in dem er den Bildschirm mit einem anderen Handy oder Tablet abfotografiert. Das kann WhatsApp allerdings auch nicht verhindern.

Quelle: https://www.netzwelt.de/news/209726-whatsapp-greift-messenger-verboten-1611.html