Phishing: der neue Einbruch im Jahr 2021?

34.000.000 Euro.[1] Das ist der Gesamtbetrag, den Phisher im Jahr 2020 stehlen konnten. Was ist Phishing und wie gehen diese Cyberkriminellen vor? Bekomme ich mein Geld zurück, wenn ich betrogen wurde und wie erkenne ich gefälschte E-Mails? Wir haben es für Sie herausgefunden.

Phishing?

Phishing ist eine Form der Cyberkriminalität, bei der das potenzielle Opfer per E-Mail, Textnachricht, soziale Medien oder Telefon angesprochen wird. Der Betrüger gibt sich als eine andere Person aus, um an die vertraulichen Daten der Opfer zu gelangen. Es ist ähnlich wie beim Internet-Betrug, nur dass der Täter nicht Daten, sondern Menschen manipuliert. Es ist eine Form der Psychologie, auf diese Weise das Vertrauen des Opfers zu gewinnen. Phisher arbeiten sehr raffiniert und antizipieren geschickt aktuelle Ereignisse. Nachrichten von einer Bank, einem Technologieunternehmen oder einem Postdienst, die besagen, dass ein Paket auf Sie wartet, die Wahrscheinlichkeit, dass Sie eine dieser Nachrichten erhalten haben, ist sehr hoch.

[1] https://www.febelfin.be/nl/press-room/phishing-2020-de-cijfers

Federale Overheidsdienst FINANCIEN

Geachte heer/mevrouw,

Op 16 oktober heeft de overheid besloten om elk huishouden een bedrag van €202,68 toe te kennen ter compensatie van uw energie en waterfactuur.

Ter identificatie en controle is het van belang om een verificatie na te gaan om dit proces te vervolledigen. Vervolgens zal u het bedrag binnen enkele werkdagen ontvangen.

Wat heeft u hiervoor nodig?
- Bankkaart
- Kaartlezer

Via de onderstaande link kunt u het verificatie proces terugvinden.

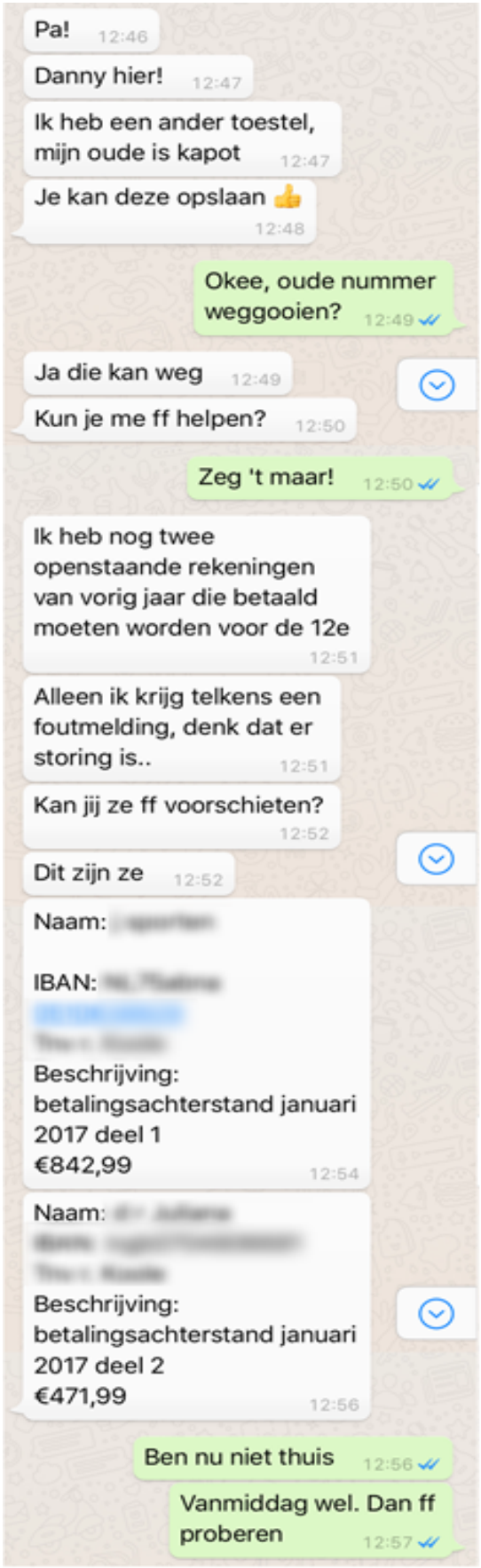
Covid-19 compensatie

Let op: Indien u de verificatie niet juist heeft volbracht, hebt u geen recht op een compensatie.

Wij vertrouwen erop u voldoende te hebben geinformeerd.

Met vriendelijke groeten,
Federale Overheidsdienst Financiën

Disclaimer Privacy Policy
Dit is een automatisch verstuurd bericht. Het is niet mogelijk om te antwoorden op dit bericht.



Das Phänomen des Phishings oder "Angelns" nach sensiblen Daten wie Passwörtern und Bank- oder Kreditkartendaten hat in den letzten Jahren exponentiell zugenommen. Im Jahr 2020 wurden nicht weniger als 3.200.000 verdächtige Nachrichten an das Centre for Cybersecurity Belgium (CCB) weitergeleitet. In der ersten Hälfte des vergangenen Jahres erstellten die Polizeidienststellen 3.438 offizielle Berichte über Phishing. Eine Vervierfachung im Vergleich zum Vorjahr. Doch das ist nur die Spitze des Eisbergs, so die Staatsanwaltschaft.[2]

Dafür gibt es verschiedene Gründe. Zum einen steigt die Zahl der Phishing-Nachrichten exponentiell an, so dass die Staatsanwaltschaft die Flut an Dateien einfach nicht mehr verarbeiten kann. Es scheint fast ein unangenehmer Nebeneffekt der Corona-Krise zu sein, dass Kontakte nun zunehmend digital geknüpft werden. Angesichts der vielen Opfer und der begrenzten personellen und finanziellen Ressourcen der Justiz ist die Chance, dass die Täter gefasst werden, eher gering.

[2] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/.

Darüber hinaus ist die Anonymität des Täters ein wichtiger Erklärungsfaktor. Sicher hinter seinem Computerbildschirm kann ein Cyberkrimineller unter dem Radar des Gesetzes Tausende Menschen gleichzeitig ausrauben, da sie in vielen Fällen nicht in der Lage sind, die Identität der Person zu ermitteln, die falsche Nachrichten verschickt oder eine gefälschte Website einrichtet. Die Täter glauben, dass sie straffrei bleiben.

Schließlich ist Phishing ein Kinderspiel. Sie müssen kein Computergenie sein, um Phishing zu betreiben. Es geht einfach darum, das Vertrauen der Opfer zu gewinnen, um sensible Informationen zu extrahieren und Geld zu stehlen.

Wie arbeiten diese Cyberkriminellen?

Ganz einfach. Phishing hat oft eine strukturierte Organisation. An der Spitze der Pyramide stehen die IT-Experten, die Softwareprogramme erstellen, mit denen sie glaubwürdige Phishing-Seiten und -E-Mails erstellen können. Durch das Hacken von Webseiten, auf denen sich Menschen registriert haben, gelangen die Betrüger an Daten, die in geschlossenen Chatgruppen über Online-Marktplätze angeboten werden. Phisher kaufen die Daten, die von den Softwareprogrammen stammen, und wählen ihre Opfer aus dieser Liste aus. Auf diese Weise können Phisher oft Tausende Personen gleichzeitig anschreiben. Ganz unten sind die Geldesel. Das Geld der Opfer, das die Phisher stehlen, landet auf deren Konten. Also eine Art Ablenkungsmanöver für die Justizbehörden, denn so bleiben nicht nur die Bandenchefs für die Ermittler oft unauffindbar, sondern auch die Phisher können kaum aufgespürt werden.

Bekomme ich mein Geld zurück?

Die vielleicht wichtigste Frage für die Opfer ist: Bekomme ich mein Geld zurück? Es ist wichtig, dass Opfer schnell handeln. Wenn Ihnen eine Transaktion doch verdächtig vorkommt, wenden Sie sich sofort an Ihre Bank. Sie können den Zugriff auf Ihre Konten sperren lassen. Die Chance, dass Sie rechtzeitig sind, scheint kleiner zu sein, da das Geld ab dem Zeitpunkt der Auftragserteilung definitiv die Bank verlassen hat. Deshalb arbeiten die Banken zusammen, um Konten so schnell wie möglich sperren zu lassen. Sobald eine Bank über einen Phishing-Fall informiert wird, nimmt die Bank des Opfers Kontakt mit der Bank des Geldkuriers auf. Mit anderen Worten: die Bank, an die das Geld überwiesen wird. Sie werden versuchen, die Gelder zu sperren und sie anschließend wieder einzuziehen.

Wenn dies nicht funktioniert und das Geld bereits verschwunden ist, besteht die Möglichkeit einer Entschädigung durch Ihre Bank zu bekommen. Dieser wird eine Interessenabwägung vornehmen, ob Sie haftbar gemacht werden können oder nicht. Hierfür verwendet die Bank die Kennzahl "große Fahrlässigkeit"[3]. Sie werden jede Situation prüfen, um zu sehen, welche Betrugstechnik verwendet wurde und ob die Kunden zu unvorsichtig waren, indem sie ihre persönlichen Daten - wenn auch unter Druck und in gutem

[3] https://www.standaard.be/cnt/dmf20210507_97478909

Glauben - an einen Cyberkriminellen weitergaben. In jedem Fall liegt die Beweislast bei der Bank und es liegt nicht an Ihnen, zu beweisen, dass Sie nicht fahrlässig waren.

Die Figur der "großen Fahrlässigkeit" ist Gegenstand heftiger Diskussionen, da das Gesetz nicht eindeutig definiert, was als "große Fahrlässigkeit" zu verstehen ist und was nicht. Testaankoop[4] ist der Meinung, dass Banken dieses Konzept immer wieder nutzen, um die Rückzahlung zu vermeiden. Beispiele für "große Fahrlässigkeit" sind, dass Sie Ihre Bankkarte nicht sperren oder die Karte nicht zusammen mit dem Code aufbewahren oder sie niemandem anvertrauen. Aber es ist sehr schwierig, hier eine allgemeine Linie zu ziehen. In der Praxis erstatten viele Banken dem Kunden in vielen Fällen Geld zurück.[5]

Wenn die Bank die volle Verantwortung übernimmt und Sie sich als Opfer fühlen, zögern Sie nicht, Ihren Konflikt an Ombudsfin[6], die Schlichtungsstelle für Finanzstreitigkeiten, zu richten. Dies ist eine unabhängige Institution, die bei Streitigkeiten über betrügerische Transaktionen und Erstattungen zwischen dem Opfer und der Bank vermitteln kann.

Wie erkenne ich falsche Meldungen?

Phisher sind sehr erfinderisch und erfinden regelmäßig neue Tricks, um Menschen um Geld oder Daten zu betrügen. Außerdem werden die Betrugsmethoden immer schwieriger zu erkennen. Die Unterscheidung zwischen falschen E-Mails und zuverlässigen Nachrichten scheint fast unmöglich. Im Folgenden haben wir eine Reihe von Tipps aufgelistet, um zu beurteilen, ob Sie einer Nachricht vertrauen können.

Zweifeln Sie daran, dass eine Meldung verdächtig ist? Dann beantworten Sie diese Fragen kurz für sich selbst:[7]

1. Ist es unerwartet?
2. Ist es dringend?
3. Kennen Sie den Absender?
4. Finden Sie die Frage seltsam?
5. Wohin führt der Link, den Sie anklicken sollen? Tipp: Fahren Sie mit dem Mauszeiger über den Link und sehen Sie, wohin er Sie führt. Öffnen Sie einen
6. Werden Sie persönlich angesprochen?

[4] https://www.test-aankoop.be/geld/betalen/dossier/betaalkaarten-hoe-krijgt-u-uw-geld-terug/dief-heeft-uw-kaart-of-gegevens.
[5] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/
[6] https://www.ombudsfin.be/
[7] https://www.safeonweb.be/nl/leer-valse-mails-herkennen

verdächtigen Link am besten nicht.

7. Enthält die Nachricht viele Sprachfehler?
8. Ist die Nachricht in Ihrem Spam?
9. Versucht jemand, Sie neugierig zu machen?

Riecht es nach einem von Ihnen getätigten Geschäft? Wenden Sie sich so schnell wie möglich an Card Stop, um Ihre Karte sperren zu lassen. Sie können dies unter der Nummer 070 344 344 tun. Bitte beachten Sie, dass Card Stop niemals Personen anrufen wird. Wenn jemand am Telefon vorgibt, ein Mitarbeiter von Card Stop zu sein, ist diese Person 100% sicher ein Betrüger.

Es ist auch wichtig, so viele Beweise wie möglich zu sammeln. Notieren Sie sich immer alle Details, die Sie von den Betrügern erhalten haben, wie z. B. Telefonnummern und Namen. Machen Sie ggf. Screenshots von den gefälschten E-Mails, Links und der Website. Mit diesen Beweisen können Sie problemlos eine Anzeige bei der Polizei erstatten und einen offiziellen Bericht erstellen lassen.

Geben Sie schließlich niemals persönliche Codes wie Ihre PIN-Nummer oder Ihren Antwortcode an. Die Bank wird niemals auf irgendeinem Weg nach diesen Codes fragen. Im Allgemeinen sollten Sie nicht zu naiv sein. Eine Nachricht, die zu schön ist, um wahr zu sein, ist es meistens auch. Darüber hinaus spielen Phisher oft mit dem Gefühl, dass es schnell gehen muss. Seien Sie also wachsam für Nachrichten, die eine gewisse Dringlichkeit hinter sich haben. Glauben Sie nicht blind jeder E-Mail oder Textnachricht, aber glauben Sie auch nicht, dass es Ihnen nie passieren wird. Seien Sie auf der Hut und prüfen Sie doppelt!

Wenn Sie beim Surfen im Internet auf eine verdächtige Nachricht stoßen, zögern Sie nicht, sie an verdacht@safeonweb.be weiterzuleiten. Sie prüfen die Links und Anhänge dieser weitergeleiteten Nachrichten und sind in der Lage, verdächtige Links zu blockieren. Auf diese Weise werden auch weniger aufmerksame Internetnutzer, die auf den Link geklickt haben, geschützt. Durch schnelles Handeln wird die Chance, dass Cyberkriminelle Opfer finden, verringert. Eine Warnung ist zwei wert.

Wenn Sie nach dem Lesen dieses Artikels noch Fragen zum Thema Phishing haben, zögern Sie nicht, uns über joost.peeters@studio-legale.be, simon.geens@studio-legale.be oder 03 216 70 70 zu kontaktieren.