

PHISHING, BITTE NICHT ANBEISSEN

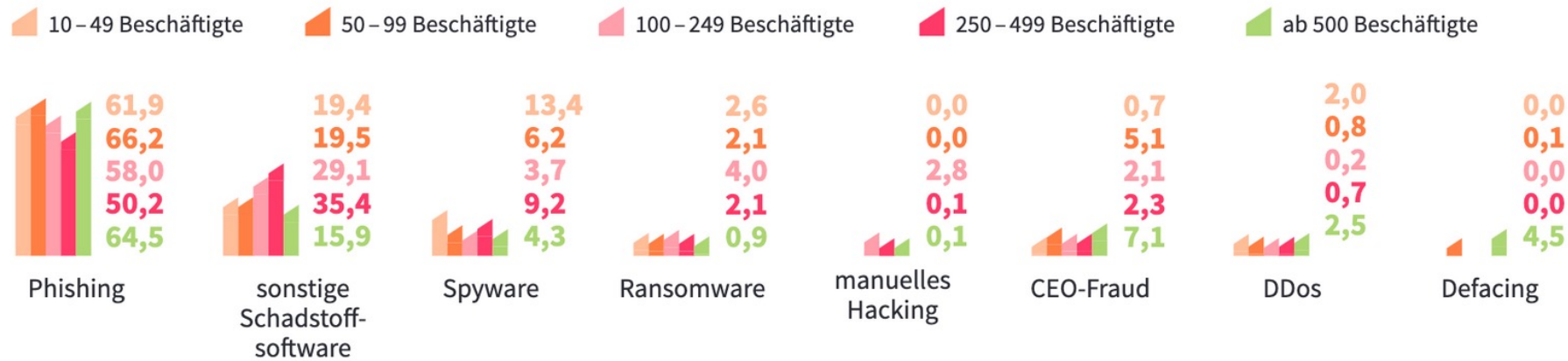
Moritz Samrock

DIGITALE SICHERHEIT
ANPACKEN

#umsetzungstag

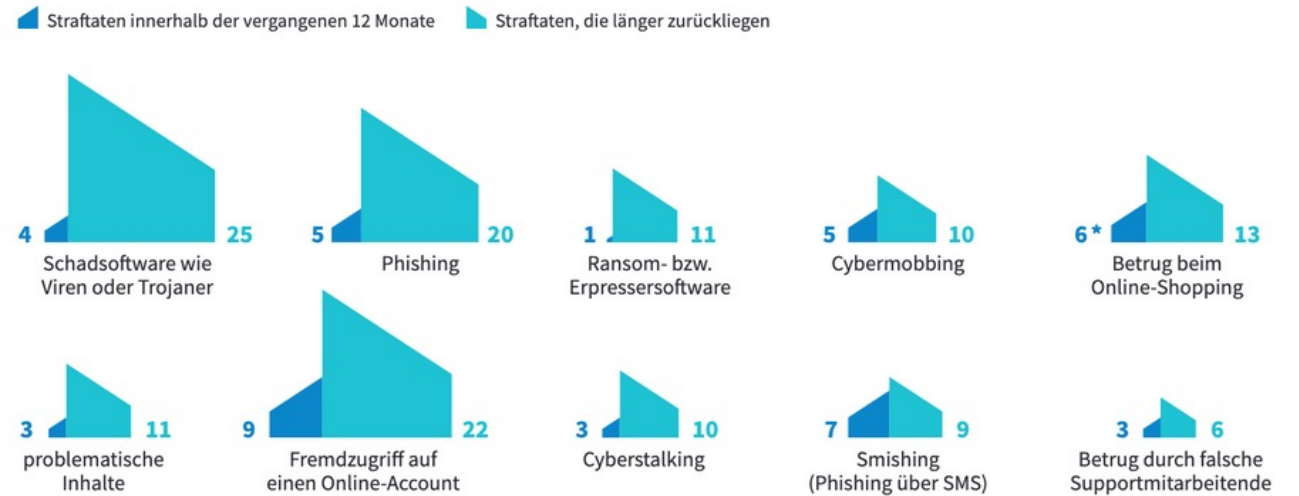


Anteil der erlebten Cyberangriffe nach Angriffsart und Beschäftigtengrößenklassen; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; 2020; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Opfer von Internetkriminalität nach Art der Straftat; Befragte, die Opfer von Internetkriminalität geworden sind; Deutschland; 2021; in Prozent



* Kleine Fallzahl (insgesamt 94 Opfer beim Online-Shopping).
 Quellen: Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)

PHISHING

Phishing

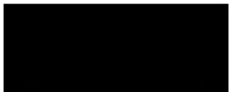
A close-up photograph of a computer keyboard. The central focus is a single key with the word "Phishing" printed on it in a serif font. The key is a light beige color and is surrounded by other keys, some of which are partially visible. The lighting is dramatic, with strong highlights and deep shadows, creating a sense of depth and texture. The overall color palette is dominated by light beige and dark shadows, with a slight blue tint in the background.



Sehr geehrte/r [REDACTED]

Ihre persönlichen Daten bedürfen der Aktualisierung. Sie sind verpflichtet, Ihre Daten bei Aufforderung zu aktualisieren. Sollten Sie Ihre Daten nicht innerhalb der nächsten 14 Tage fristgerecht bis zum 01.08.2019 aktualisiert haben, werden wir Sie schriftlich per Einschreiben zur Aktualisierung auffordern. Hierbei kann ein Entgelt von 2,56 Euro entstehen.

Aktuelle Versandadresse:



[Zur Aktualisierung](#) 

Wichtiger Hinweis:

Sollte Ihre aktuelle Versandadresse abweichen und dort ein Formblatt zusammenfügen

Freundlich grüßt

Hallo [REDACTED]

Durch eine Sicherheitslücke in deinem System konnte ich unbemerkt einen Virus auf deinem Gerät installieren. Aufgrund dieses Virus hab ich kompletten Zugriff auf dein System. Ich hab versteckt auf deiner Festplatte Kinderpornos gespeichert, sowie ein Sicherheitskopie deiner persönlichen Daten(z.B Deine Anschrift und Bankdaten),Fotos & Videos erstellt. Solltest du mir nicht glauben hier ein Parr Beispieldaten:

Name: [REDACTED]
Geburtsdatum: [REDACTED]
Adresse: [REDACTED]
PLZ / Stadt: [REDACTED]
Bank: [REDACTED]
IBAN: [REDACTED]

Als du dich das Letzte mal selbstbefriedigt hast, hab ich mithilfe des Virus ein Video aufgezeichnet. Auf diesem Video ist zusehen, wie du masturbierst, ich hab durch gekonnte Bearbeitung das Video so verändert, das man im Vordergrund siehst, wie Du masturbierst und im Hintergrund("Deinem Bildschirm") Sieht man wie Du dir Kinderpornos anguckst, Du und ich wissen das es sich dabei um ein "Fake" handelt, Aber stell dir vor was passiert, wenn ich das Video veröffentliche, es an die Polizei weiterleite. Die Polizei wird eine Hausdurchsuchung bei dir durchführen und wird die gespeichert Kinderpornos finden, du wirst ein verurteilter Kinderschänder sein. Deine Freunde und Familie werden sich von dir abwenden, du wirst dein Job verlieren. Niemand wird etwas mit dir zutun haben wollen.

Als du diese E-Mail geöffnet hast, hat sich automatisch ein Timer gestartet, Du hast ab jetzt 72 Stunden zeit 750€ in Bitcoin an die nachfolgende Bitcoin Adresse("Bitcoin Wallet") zu zahlen: [REDACTED]

Sollte die Zahlung in dieser Frist nicht eingehen, wird das Video automatisch veröffentlicht, es wird an deine Freunde und Familie weitergeleitet und außerdem wir anzeige bei der Polizei erstattet.

Solltest du aber wie gefordert zahlen, wird sich das Video automatisch Löschen, die Kinderpornos werden von deiner Festplatte gelöscht und du wirst nie wieder von mir Höhren.

Wenn du nicht weißt, wie du an Bitcoins kommst bzw. wie du dies kaufen kannst, ich helfe dir da gerne bei. Es ist ganz einfach, du gehst einfach auf google und suchst nach einen der beiden Sätze"Wie Kauf ich Bitcoins" oder "How to Buy Bitcoins"

[REDACTED] das ist kein Scherz, solltest du die 750€ nicht bezahlen werde ich deine leben zerstören, Ich werde nicht aufhören bis du alles verloren hast und als Kinderschänder abgestempelt bist, es liegt in deiner Hand.

Sehr geehrte Damen und Herren,

leider kam es in letzter Zeit vermehrt zu Problemen mit den hinterlegten Kontaktdaten unserer Kunden, daher bitten wir sie ihre bereits hinterlegten angaben in unserem Kundencenter abzugleichen.

Um einer vorsorglichen Abgleichs Sperrung ihres Kontos unsererseits entgegenzuwirken, empfehlen wir ihnen den Abgleich schnellstmöglich selbst durchzuführen.

ir einfach auf »Zum Formular« und folgen en Anweisungen die ihnen im Kundencenter en.

i Grüßen,
Volksbanken-Raiffeisenbanken

[»Zum Abgleich«](#)

Hallo [REDACTED]



hilfe ist erforderlich!

utzgesetzte verpflichten uns nun dazu, itänden die Konten unserer Kunden zu ent ausschließlich zu Ihrer eigenen 'Vergangenheit immer mehr Vorfälle chiedener Kundenkonten durch i entstanden sind.

nt weiterhin Ihr Konto bei uns nutzen zu : **Mitwirkung erforderlich. Dies wird vom ght.**

r den Bestätigungsbutton angemeldet detailliert alle weiteren notwendigen Schritte

[Bestätigen](#)

Bei Misachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

Mit freundlichen Grüßen
Ihr PayPal Kundensupport

Von Infektionsinformation Bundesgesundheitsministerium <infizierten-information@bundesgesundheitsministerium.de> ☆
Betreff **WICHTIG: Infektion im Bekanntenkreis mit Covid-19 (Coronavirus)** 13:52
An [REDACTED] ★

Sehr geehrte/r [REDACTED],


in Ihrem Bekanntenkreis ist ein Verdachtsfall des Virus CoVid-19, besser bekannt als Coronavirus, aufgetreten.

Aus diesem Grund fordern wir Sie auf, sich unverzüglich auf der extra eingerichteten [Online-Meldestelle des Bundesministeriums für Gesundheit](#) zu registrieren.

Dabei handelt es sich um eine reine Vorsichtsmaßnahme, um die Infektionsketten und deren Verlauf nachvollziehen zu können. Auf diese Weise können weitere Maßnahmen getroffen werden.

Mit freundlichem Gruß

Dr. Thomas Gebhart
Parlamentarischer Staatssekretär des Bundesministers für Gesundheit
Rochusstraße 1
53123 Bonn

 **Bundesministerium
für Gesundheit**

Microsoft-Konto

Ungewöhnliche Anmeldeaktivität

Bei der Anmeldung beim Microsoft-Konto "[REDACTED]" haben wir vor Kurzem etwas Ungewöhnliches bemerkt.

Anmeldeinformationen

Land/Region: Pakistan

IP-Adresse: 149.83.224.251

Datum: Thursday 27. February 2020 17:50:01

Plattform: Windows

Browser: Microsoft Edge

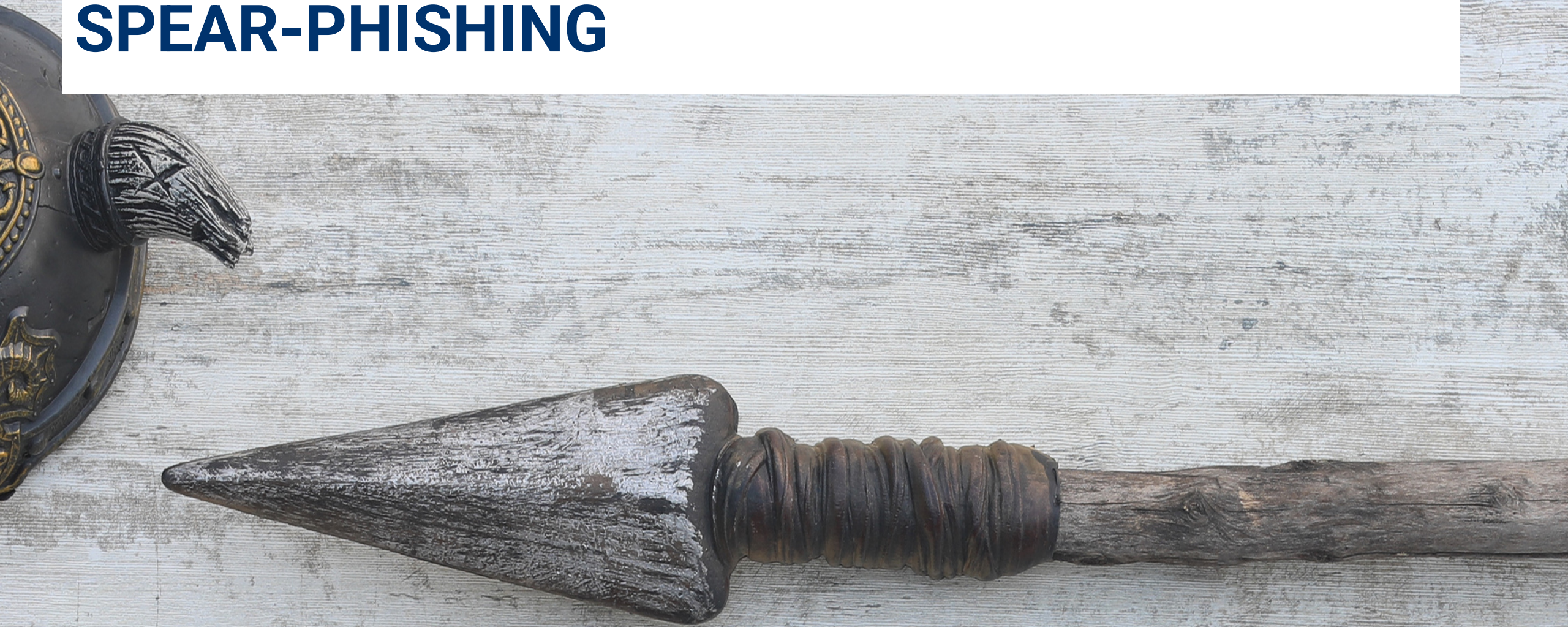
Wechseln Sie zur Seite mit den letzten Aktivitäten, und teilen Sie uns mit, ob Sie den betreffenden Vorgang durchgeführt haben. Falls dies nicht der Fall ist, helfen wir Ihnen, Ihr Konto zu schützen. Bitte überprüfen Sie die angesprochenen Aktivitäten umgehend, da es sich um einen unerlaubten Zugriff handeln könnte. Sollten Sie in den nächsten 24 Stunden keine Überprüfung vornehmen, wird ihr Konto aus Sicherheitsgründen vorübergehend gesperrt.

[Letzte Aktivität überprüfen](#)

Falls Sie keine Sicherheitsbenachrichtigungen mehr erhalten oder das Ziel für Sicherheitsbenachrichtigungen ändern möchten, [klicken Sie hier](#).

Mit freundlichen Grüßen
Ihr Microsoft-Konto-Team

SPEAR-PHISHING





Liebe Mitarbeiter der [REDACTED],

[REDACTED] hat in Zusammenarbeit mit Corporate Benefits einen tollen Deal für seine Mitarbeitenden herausgeschlagen!

Monatlich können von Ihrem Arbeitgeber 44€ steuerfrei auf Ihr Amazonkonto überwiesen und ohne Einschränkungen genutzt werden. Wenn Sie diesen Deal nutzen wollen, registrieren Sie mit dem Konto, auf dem das Guthaben genutzt werden soll. Rufen Sie dazu die Seite [Vorteile sichern](#) auf und klicken Sie auf "Registrieren".

Vorteile sichern!

CB_Amazon_ID #302-02890255-5698943

Dies ist eine automatisch versendete E-Mail. Bitte antworten Sie nicht auf diese Nachricht, da die E-Mail-Adresse nicht zum Empfang von E-Mails eingerichtet ist.

From: Sandra Homes [<mailto:attend3@attendeed.tech>]
Sent: 12 July 2023 08:41
To: 'info@laakoon-security.com'
Subject: Digital Demo Day
Importance: High

Dear Exhibitors,

This is regarding **Digital Demo Day 2023** –Attendees list is available now

You can use this list for your booth invitation, pre-show marketing campaigns, appointment setting.

Just pick the number that describes best of your response.

Yes – Interested in counts and pricing details

No – Take off

Sincerely,
Sandra Homes
Event and Trade Show Coordinator



Liebe Kolleginnen und Kollegen,

auch dieses Jahr möchten wir wieder ein rauschendes Sommerfest feiern. Hierzu sind die Planungen bereits in vollem Gange. Wir möchten es jedoch nicht verpassen, Euch in die Planung mit einzubeziehen!

Um Euch diese Möglichkeit zu bieten, bitten wir darum, eure Wünsche bzgl. Menü und Aktivitäten in das angehängte Word-Dokument einzutragen. Anschließend reicht es, wenn Ihr die Datei [hier](#) hochladet. Auf diese Weise können die Vorschläge anonymisiert gesammelt und ausgewertet werden. Fühlt euch also frei! Wir freuen uns auf Euer Input!

Viele Grüße

Euer Sommerfest Organisationsteam

WHALING



Falsche Überweisung nach Polen

Dass auch eine öffentliche Einrichtung auf eine Betrugsmasche hereinfliegen kann, musste der Fonds du Logement erfahren. Es geht um immerhin 800.000 Euro.



Foto: LW-Archiv/Pierre Matgé



22.01.2019

(TJ/rc) - Nicht weniger als 800.000 Euro hat der Fonds de Logement auf ein falsches Konto in Polen überwiesen und ist damit aller Wahrscheinlichkeit nach auf eine Betrugsmasche hereingefallen. Dies meldet RTL am Dienstag.

Das Geld war für eine Baufirma bestimmt, die für den staatlichen Wohnungsbauträger Arbeiten erledigt hatte. Der Fonds erhielt eine E-Mail mit der Aufforderung, das Geld - 800.000 Euro - auf ein polnisches Konto der Firma zu überweisen.

AUF CHEF-TRICK REINGEFALLEN

Bäckerei-Angestellte überweist 1,9 Millionen Euro an Trickbetrüger



Filiale einer Hopfister-Bäckerei

© DPA/picture alliance

15.07.2017, 14:31 • 2 Min.

MERKEN

Sie dachte, die Anweisung käme von der Chefin, stattdessen überwies die Buchhalterin einer Münchner Bäckereikette 1,9 Millionen Euro an Trickbetrüger aus Hongkong. Nun wird vor Gericht gestritten, wer den Schaden bezahlen muss.

Auf E-Mail reingefallen: Landesministerium überweist Kriminellen 225.000 Euro

Sachsens Gesundheitsministerium hat eine betrügerische Rechnung bezahlt und Kriminellen 225.000 Euro überwiesen. Vor der Masche hat das LKA schon 2016 gewarnt.

Lesezeit: 2 Min.  In Pocket speichern

   284



(Bild: SOMKKU/Shutterstock.com)

Norwegens Vermögensfonds verliert 10 Millionen Dollar durch Datenmissbrauchs

Am 13. Mai gab [Norfund bekannt](#), dass er „eng mit der Polizei und anderen zuständigen Behörden zusammenarbeitet“, nachdem „eine Reihe von Ereignissen“ Betrügern erlaubt hatte, sich mit 10 Millionen Dollar davonzumachen.

Der Fonds gab an, dass ein Datenbruch Betrügern den Zugang zu Informationen über ein Darlehen von 10 Millionen US-Dollar von Norfund an eine Mikrofinanzinstitution in Kambodscha ermöglichte.

Mit Hilfe einer Mischung aus manipulierten Daten und gefälschten Informationen gelang es den Betrügern, sich als das kreditgebende Institut auszugeben und Gelder vom echten Empfänger in die eigene Tasche abzuzweigen.

„Die Betrüger manipulierten und fälschten den Informationsaustausch zwischen Norfund und der kreditgebenden Institution im Laufe der Zeit auf eine Weise, die in Struktur, Inhalt und Sprachgebrauch realistisch war. Dokumente und Zahlungsdetails wurden gefälscht“, sagte ein Norfund-Sprecher.

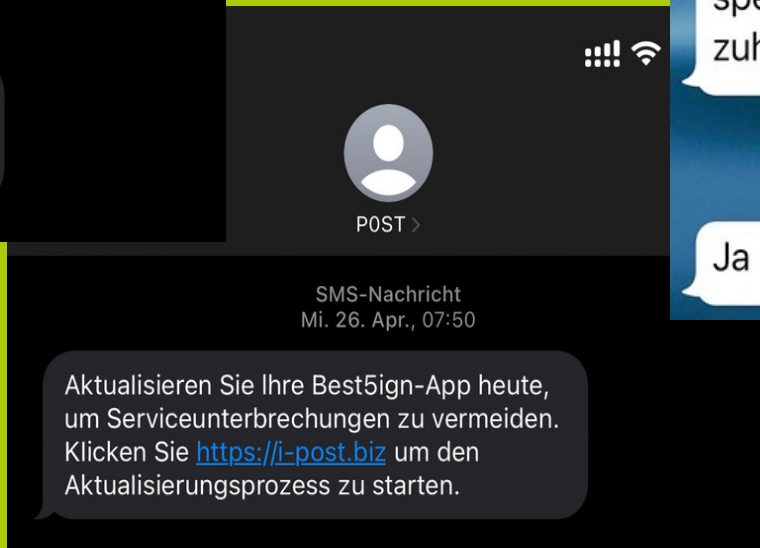
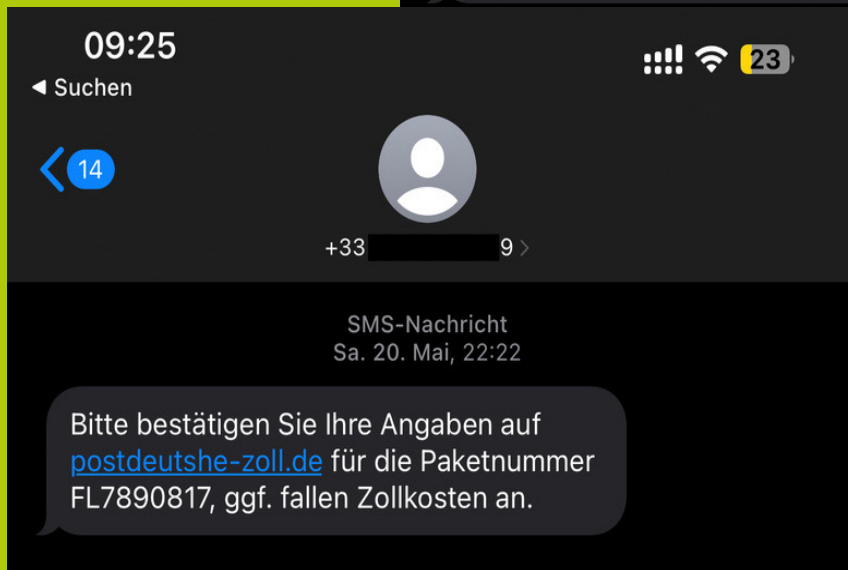
Gelder wurden auf ein Konto in Mexiko umgeleitet, das auf den gleichen Namen wie die kambodschanische Mikrofinanzinstitution lautet. Der Diebstahl fand am 16. März statt, blieb aber bis zum 30. April unentdeckt, als die Betrüger versuchten, auf betrügerische Weise mehr Geld zu erhalten.

SMISHING

+49 [REDACTED] 8 >

SMS-Nachricht
Heute, 16:33

Hallo Papa oder Mama, das ist meine neue nummer, kannst du mir eine nachricht auf WhatsApp schicken [015 \[REDACTED\] 68](tel:015-[REDACTED]-68) wenn du das siehst



VISHING

Unknown Caller
VISHING **ALERT**

Don't share your bank data



Windows wurde a blockiert

Bitte aufhören und den PC nicht schließen



**Rufen Sie uns an:
0711-49-05-07-29**

Kontaktieren Sie unsere
technische Abteilung direkt

**Instant ohne auf
Hilfe zu warten**

Benannt 0711-49-05-07-29
(San.rais) und Gesundheit
verbessern. Ihr Computer

**Updates mit
Fenstern**

Unsere professionals halten Sie
auf dem Laufenden mit der
neuesten Software

**Erfahren Sie mehr
über den sicheren
Browser**

Erfahren Sie mehr über den
sicheren Versand für
Informationen 0711-49-05-07-29

Bitte rufen Sie uns an: 0711-49-05-07-29 (Ohne Gebühr)

Anmelden

http://www.winhelpde.club

Die Verbindung zu dieser Website ist nicht sicher

Nutzername

Passwort

Abbrechen Anmelden

Authentifizierung erforderlich

http://www.win-firefox-help-jp.club Ich ersuche Ihren Benutzernamen und Ihr Passwort.

Warnung: Passwörter werden nicht an die Website gesendet, die Sie gerade besuchen.

Website Edition: *Ihr Computer ist gesperrt, um Ihren Computer sicher zu machen, Hotline-Nummer

Nutzername:

Passwort:

OK Stornieren



Nu Html Checker

This tool is an ongoing experiment in better HTML checking, and its behavior remains subject to change

Showing results for contents of text-input area

Checker Input

Show source outline image report

Check by CSS

Kreditkartennummer: 1234 5678 9876 5432

Use the Message Filtering button below to hide/show particular messages, and to see total counts of errors and warnings.

Message Filtering

- Warning** Consider adding a `lang` attribute to the `html` start tag to declare the language of this document.
From line 1, column 1: to line 1, column 38
Kreditkartennummer: 1234 5678 9876 5432
For further guidance, consult [Declaring the overall language of a page](#) and [Choosing language tags](#).
If the HTML checker has misidentified the language of this document, please [file an issue report](#) or [send e-mail to report the problem](#).
- Error** Non-space characters found without seeing a doctype first. Expected `<!DOCTYPE html>`.
From line 1, column 1: to line 1, column 38
Kreditkartennummer: 1234 5678 9876 5432
- Error** Element `head` is missing a required instance of child element `title`.
From line 1, column 1: to line 1, column 38
Kreditkartennummer: 1234 5678 9876 5432
Content model for element `head`:
If the document is an [iframe srcdoc document](#) or if title information is available from a higher-level protocol: Zero or more elements of [metadata](#)
Otherwise: One or more elements of [metadata content](#), of which exactly one is a [title](#) element and no more than one is a [base](#) element.

Document checking completed.

Source

- Kreditkartennummer: 1234 5678 9876 5432

Used the HTML parser.

Total execution time 2 milliseconds.

Event Viewer (Local) System Number of events: 5,186

Level	Date and Time	Source	Event ID	Task Category
Error	12/7/2015 12:30:56 AM	Service Control Manager	7031	None
Error	12/7/2015 12:30:58 AM	DistributedCOM	10010	None
Error	11/20/2015 10:48:17 AM	Service Control Manager	7031	None
Error	11/30/2015 9:43:53 AM	Schannel	36888	None
Error	11/20/2015 10:48:17 AM	Service Control Manager	7031	None
Error	11/20/2015 10:48:19 AM	DistributedCOM	10010	None
Error	11/20/2015 10:48:17 AM	Service Control Manager	7031	None
Error	11/20/2015 10:48:17 AM	Service Control Manager	7031	None
Error	10/27/2015 5:23:00 PM	Service Control Manager	7000	None
Error	10/27/2015 5:23:00 PM	Service Control Manager	7000	None
Error	10/27/2015 5:23:02 PM	Service Control Manager	7000	None
Error	10/12/2015 7:35:04 AM	Service Control Manager	7023	None
Error	10/27/2015 5:23:00 PM	Service Control Manager	7000	None
Error	10/27/2015 5:23:00 PM	Service Control Manager	7000	None
Error	10/27/2015 5:28:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/27/2015 5:33:02 PM	Service Control Manager	7000	None
Error	10/12/2015 7:39:03 AM	Service Control Manager	7031	None
Error	10/12/2015 7:39:03 AM	Service Control Manager	7031	None
Error	10/27/2015 5:17:47 PM	Service Control Manager	7000	None
Error	10/12/2015 7:39:04 AM	DistributedCOM	10010	None
Error	10/12/2015 7:39:03 AM	Service Control Manager	7031	None
Error	10/12/2015 7:39:03 AM	Service Control Manager	7031	None
Error	10/27/2015 5:18:00 PM	Service Control Manager	7000	None
Error	10/27/2015 5:23:00 PM	Service Control Manager	7000	None

10 WIRKSAME TIPPS GEGEN PHISHING

1. Nutzung von DNS-Einträgen wie DMARC, SPF & DKIM, um das Spoofing von E-Mail-Absendern zu verhindern
2. Nutzung von kryptographischen Signaturen und Verschlüsselung von E-Mails, z.B. durch die Nutzung von S/MIME
3. Nutzung von Passwortmanagern, die das Ziel einer Eingabe prüfen
4. Unternehmensweites Deaktivieren von Makros – Alternative: Makros signieren
5. Einsatz von intelligenten E-Mail-Filtern

10 WIRKSAME TIPPS GEGEN PHISHING

6. Etablieren Sie eine Kultur des Bewusstseins für die Gefahren von Phishing durch regelmäßige Schulungen der Mitarbeitenden.
7. Definieren Sie feste Ansprechpartnerinnen oder Ansprechpartner, die im Falle des Falles zur Verfügung stehen und schnell reagieren können.
8. Fördern Sie eine offene Fehlerkultur, indem Sie Fehler konstruktiv nachbereiten und nicht einfach bestrafen.
9. Fragen Sie im Zweifel sowohl intern als auch auf einem unabhängigen Kanal bei der Absenderin bzw. dem Absender einer potenziellen Phishing-E-Mail nach, ob Inhalt und Plausibilität stimmen.
10. Klicken Sie nicht auf Links in E-Mails oder Nachrichten, die Ihnen bereits verdächtig vorkommen.

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

Die Grundlagen der Digitalen Sicherheit sind nicht aufwändig in der Umsetzung, aber wirkungsvoll für den Schutz Ihrer Digitalen Daten und Wertgegenstände.

Besuchen Sie unsere Website: www.digital-sicher.nrw

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

 +49 234 - 5200 7334

 info@digital-sicher.nrw

Social Media



**DIGITAL
SICHER
NRW**