Sichere E-Rechnungen und E-Mails – So schützen Sie sich vor Betrug und Manipulation

BIHK-Reihe zu IT-Sicherheit

IHK

Ihr Gastgeber

Bernhard Kux

Referent für Cybersicherheit, digitale Infrastruktur, Digitalisierung

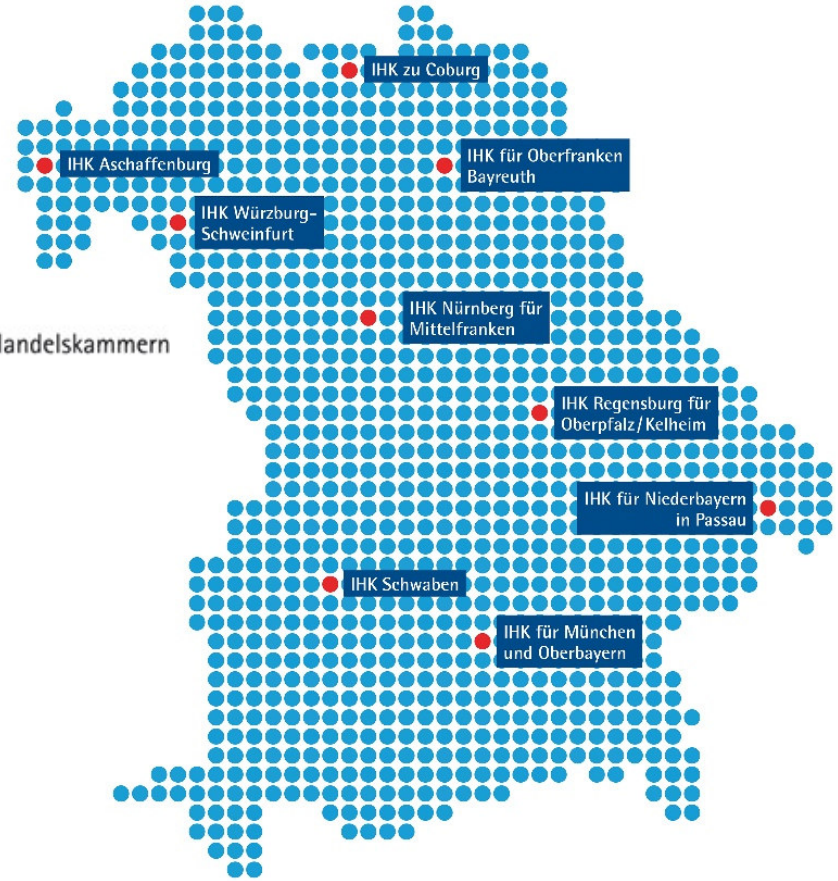
089-5116 1705
kux@muenchen.ihk.de
https://www.linkedin.com/in/bernhardkux/

BIHK-Reihe: Schutz statt Schaden – Praxisnahe Lösungen für Unternehmen

Mai	• 06.05.:	E-Rechnungen - E-Mails
	• 08.05.:	Cyber Threat Intelligence
	• 09.05.:	Cyber Resilience Act - Hersteller
	• 15.05.:	Phishing
	• 21.05.:	KI & Cyberkriminelle
	• 26.05.:	KI & Cyberangriffe
Juni	• 05.06.:	Cyber Resilience Act - Beispiel
	• 23.06.:	Resilienz & BCM
	• 24.06.:	NIS 2
Juli	• 03.07.:	Live Hacking
	• 08.07.:	KI: Wie sichern Sie Ihre Daten?
	• 15.07.:	Angriffspunkte auf Produktions- und Energiesysteme

https://www.bihk.de/itsicherheit

BIHK-Reihe IT-Sicherheit



IHK Industrie- und Handelskammern in Bayern

https://www.bihk.de/itsicherheit

Digitalimpulse im Rahmen des bayerischen Pakts für berufliche Weiterbildung

Kooperation von:

IHK Industrie- und Handelskammern in Bayern

Bayerisches Staatsministerium für Digitales

https://www.kommweiter.bayern.de/mit-unterstuetzung/pakt-fuer-berufliche-weiterbildung/

und

https://www.bihk.de/itsicherheit

Unterstützer

DIHK Deutsche Industrie- und Handelskammer

Sicherheitsnetzwerk München

bayern innovativ Digitalisierung

STE WERK18® Weichen in die digitale Zukunft

ITSECURITY www.it-sicherheitscluster.de

ROSIK e.V.

NL Niederlande

Allianz für Cyber-Sicherheit Multiplikator

Weitere Angebote:

Die IHK-Digitalisierungsinitiative „Pack ma‘s digital“

Ratgeber, Veranstaltungen, Downloads und mehr

Webseite: www.packmasdigital.de

Pack ma´s digital

Gemeinsam in die digitale Zukunft

Webinarreihe: Online-Marketing

Webseite: http://www.bihk.de/onlinemarketing

Nächster Termin: Mit KI zu professionellen LinkedIn-Beiträgen

7. Mai, 10:00 - 11:00 Uhr

PROGRAMM

11.00 Uhr	**Intro** Bernhard Kux, IHK für München und Oberbayern
11.05 Uhr	**Grußwort** Dr. Fabian Mehring, MdL, Bayerischer Staatsminister für Digitales
11.10 Uhr	**Überblick E-Rechnungen & IT-Sicherheit** Bernhard Kux, IHK für München und Oberbayern
11.30 Uhr	**E-Mail-Postfach absichern: DKIM, SPF und DMARC** Tino Hager, mailtower.app
11.50 Uhr	**Antworten auf Ihre Fragen**
12.00 Uhr + X	**Webinarende**

Grußwort

Dr. Fabian Mehring, MdL, Bayerischer Staatsminister für Digitales

Bayerisches Staatsministerium
für Digitales

Ziel des Webinars

Nach dem Webinar wissen Sie…

- …was eine E-Rechnung ist
- …welche Transportmöglichkeiten es für E-Rechnungen gibt
- …warum man (E-)Rechnungen (per E-Mail) besonders genau prüfen sollte
- …was man sofort tun kann, um die E-Mailsicherheit von sich und anderen zu verbessern
- …wie man sich auf IT-Notfälle vorbereiten kann

Überblick

E-Rechnungen & IT-Sicherheit

- Grundlagen der IT-Sicherheit für digitale Rechnungsprozesse
- E-Rechnungen per E-Mail: Spam, Betrug oder echt?
- Maßnahmen gegen den Versand gefälschter Rechnungen in Ihrem Namen
- Schutzmechanismen gegen betrügerische E-Rechnungen
- Notfallmaßnahmen: Was tun bei Betrugsfällen? Wer hilft?
- Alternativen zur E-Mail für den sicheren Empfang von E-Rechnungen

Grundlagen der IT-Sicherheit für digitale Rechnungsprozesse

Mindestnotwendigkeiten für Ihre IT-Sicherheit

- Jemand **kümmert** sich aktiv und mit passenden Ressourcen um die IT-Sicherheit im Unternehmen

- Strukturierte Wege für mehr IT-Sicherheit: **Technik + Organisation**
  - Kleinere Unternehmen: „BSI-CyberRisikoCheck nach DinSpec 27076“
  - Größere Unternehmen: „ISO27001“ oder „BSI-IT-Grundschutz“

E-Rechnung: Dateiformat?

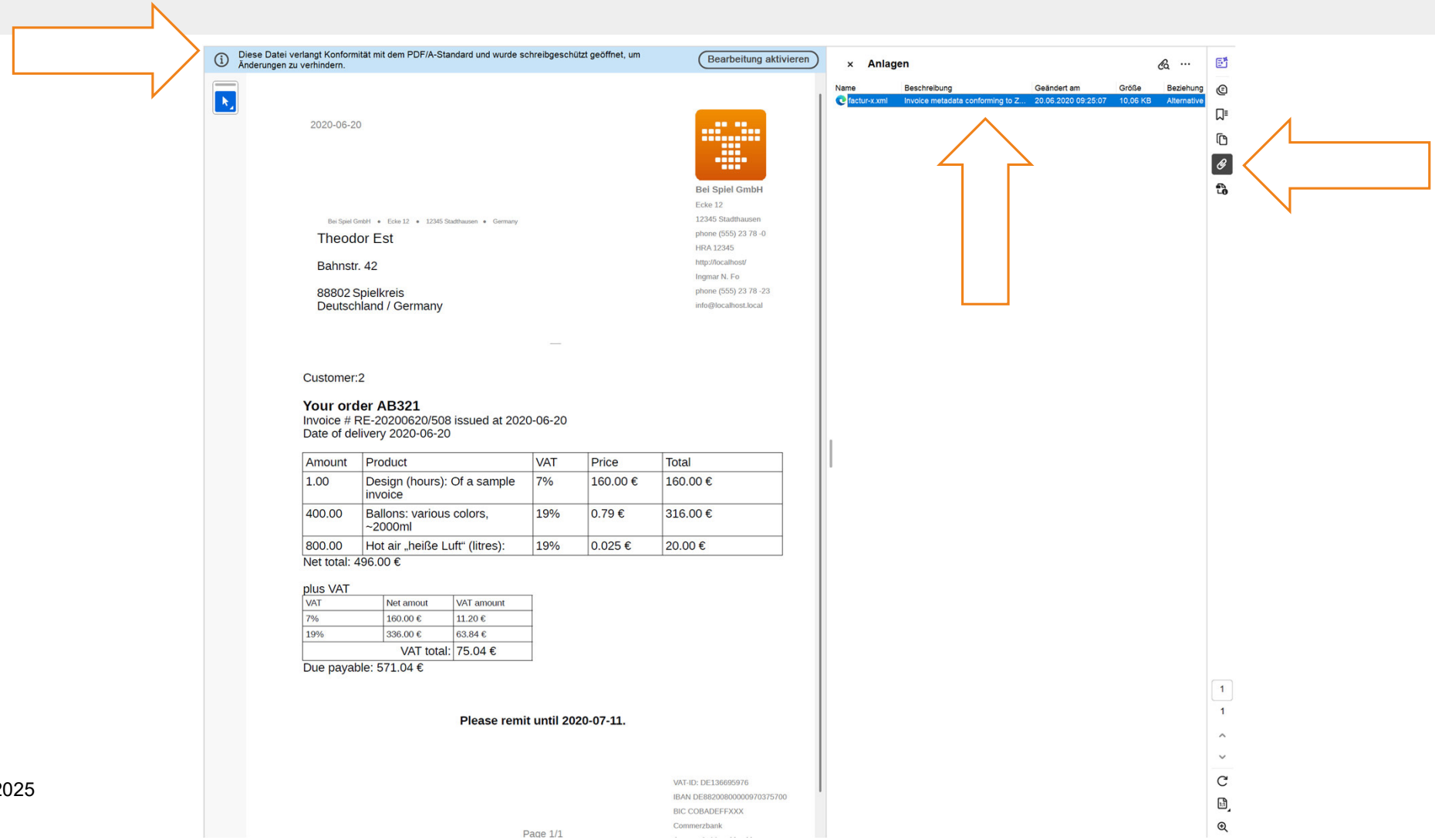
- Zwei Formate:

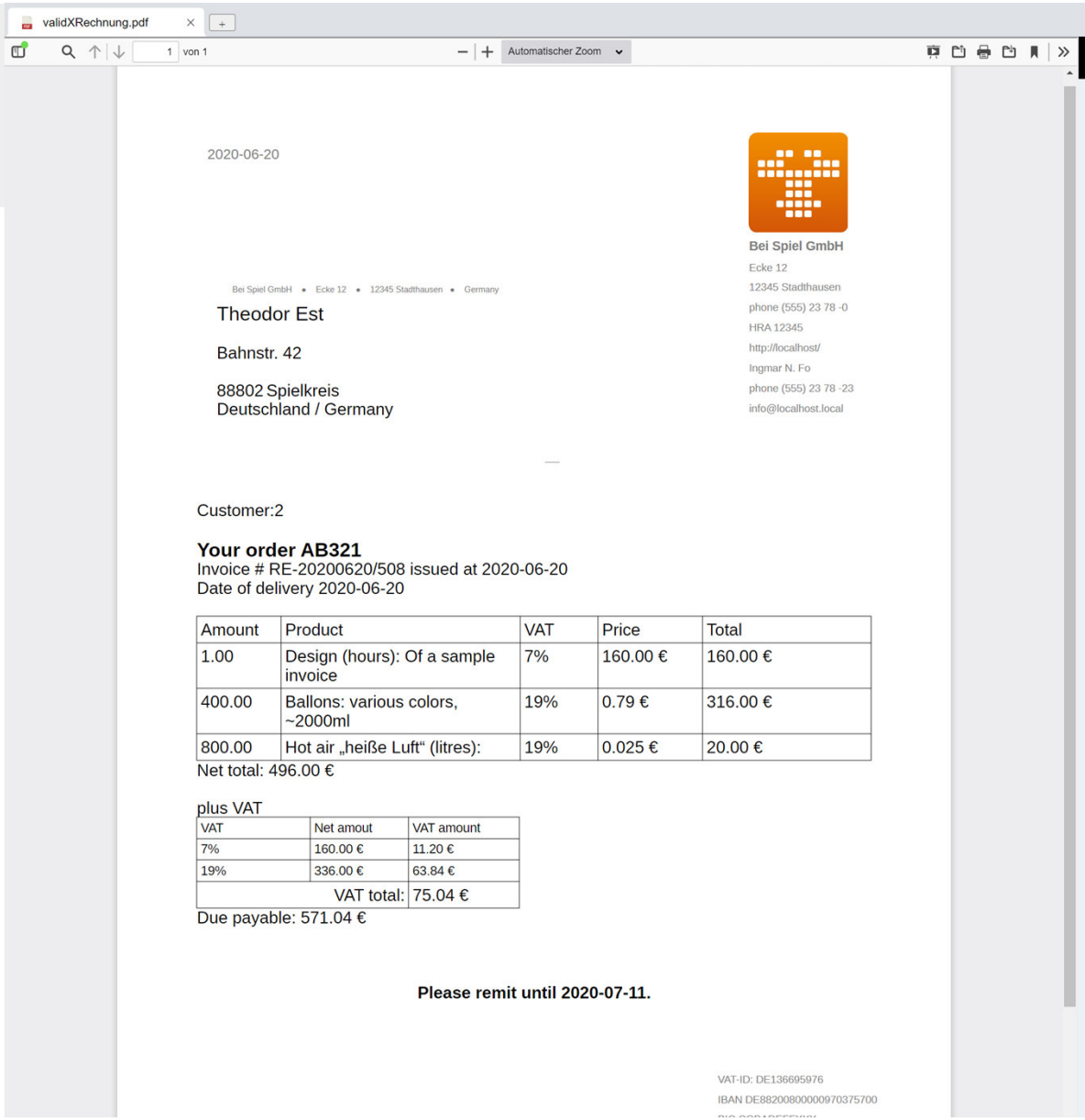
– **XML-Datei**
Textdatei

– **PDF-Datei mit integrierter XML-Datei**
PDF/A-3
ZUGFeRD (“*Zentraler User Guide des Forums elektronische Rechnung Deutschland*“)

– **Rechtlich gültig: XML-Daten**

Grundlagen der IT-Sicherheit für digitale Rechnungsprozesse




validXRechnung.pdf

1 von 1

Automatischer Zoom

2020-06-20

Bei Spiel GmbH
Ecke 12
12345 Stadthausen
phone (555) 23 78 -0
HRA 12345
http://localhost/
Ingmar N. Fo
phone (555) 23 78 -23
info@localhost.local

Bei Spiel GmbH • Ecke 12 • 12345 Stadthausen • Germany

Theodor Est

Bahnstr. 42

88802 Spielkreis
Deutschland / Germany

Customer:2

Your order AB321
Invoice # RE-20200620/508 issued at 2020-06-20
Date of delivery 2020-06-20

Amount	Product	VAT	Price	Total
1.00	Design (hours): Of a sample invoice	7%	160.00 €	160.00 €
400.00	Ballons: various colors, ~2000ml	19%	0.79 €	316.00 €
800.00	Hot air „heiße Luft“ (litres):	19%	0.025 €	20.00 €

Net total: 496.00 €

plus VAT

VAT	Net amout	VAT amount
7%	160.00 €	11.20 €
19%	336.00 €	63.84 €
	VAT total:	75.04 €

Due payable: 571.04 €

Please remit until 2020-07-11.

VAT-ID: DE136695976
IBAN DE88200800000970375700

Overview Items Information Attachments History

We accept no liability for the correctness of the data

Buyer Information

Routing ID:	AB321
Name:	Theodor Est
Street / house number:	Bahnstr. 42
PO Box:	
Address Addition:	
Postcode:	88802
Place:	Spielkreis
State/Province:	
Country:	DE (Deutschland)
ID:	
ID scheme:	
Name:	
Phone:	
E-mail address:	

Seller Information

Company name:	Bei Spiel GmbH
Street / house number:	Ecke 12
PO Box:	
Address Addition:	
Code postal:	12345
Place:	Stadthausen
State/Province:	
Country code:	DE (Deutschland)
ID:	
ID scheme:	
Name:	Ingmar N. Fo
Phone:	++49(0)237823
E-mail address:	info@localhost.local

Invoice details

Invoice number:	RE-20190610/507
Invoice date:	10.6.2019
Invoice type:	380 (Commercial invoice)
Currency:	EUR (Euro)

Billing period:

from:	
to:	

Project number:	
Contract Number:	
Order number:	
Order number:	

Previous invoices:

Total amounts of the invoice

E-Rechnung: Fälschungssicher?

- **Leider nein!**
  - **XML-Datei**
    Textdatei → leicht fälschbar
  - **PDF-Datei mit integrierter XML-Datei**
    Leicht herstellbar:
    https://tools.pdf24.org/de/elektronische-rechnung-erstellen
    Zusätzliche Herausforderung:
    Lesbare Daten vs. XML-Daten: Ggf. unterschiedlich!
    https://quba-viewer.org

E-Rechnungen per E-Mail: Spam, Betrug oder echt?

E-Rechnung vom Rechnungsteller zum Rechnungsempfänger transportieren

- **E-Mail (SMTP-Protokoll)**
- Schnittstellen: Electronic Data Interchange, AS2, Peppol-Netzwerk, Rest, Soap, WSDL…
- Onlineanwendung, Portale: Upload / Download

  Wichtig: Zwei-Faktor-Authentifizierung, zuverlässiger Anbieter

  Muster So setzen Sie Onlineanwendungen sicher ein
- Secure File Transfer Protocol
- Physische Medien: USB-Sticks…

E-Rechnungen per E-Mail: Spam, Betrug oder echt?

OLG Schleswig: Rechnung per unsicherer E-Mail – Absender haftet

- Firma A schickt eine Rechnung per unverschlüsselter E-Mail an Firma B.
- Die E-Mail wird abgefangen, die Kontodaten manipuliert.
- Firma B zahlt an ein falsches Konto.
- OLG: Firma A hätte sichere Übertragung nutzen müssen.
- Firma B muss nicht erneut zahlen.

https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/OLG/Presse/PI/202501Werklohnrechnung

E-Rechnungen per E-Mail: Spam, Betrug oder echt?

E-Mail als Transportweg

- 1970 erfunden - nicht für vertrauliche Informationen gedacht
- Leicht fälschbar
- Aufbau einer E-Mail:
  - „Für Menschen“: Betreff, Text und Anhänge
  - „Für Computer“: Welcher Server hat wie wann gearbeitet?
    Zusatzinformationen können mitgeschickt werden

E-Mail Sicherheit: Mißbrauch von Domains

Absender:
Domains oft nur kurz erreichbar

ihk-online@cpxl.nl

ihk@liftoffeagle.com

ihk@displacementwedding.com

ikh@ksamail.org

etc.

IHK

Sehr geehrter Unternehmer,

Diese Nachricht wurde an folgende E-Mail-Adresse versendet:

Durch aktuelle gesetzliche Bestimmungen sind Unternehmen dazu verpflichtet, die im IHK-Register hinterlegten Informationen zu prüfen und – wenn nötig – zu aktualisieren. Ziel dieser Maßnahme ist die rechtliche Absicherung und die Pflege korrekter Unternehmensdaten.

Wir bitten Sie, die Überprüfung und Aktualisierung Ihrer Daten bis spätestens **10. April 2025** vorzunehmen. Bei Ausbleiben der Aktualisierung kann es zu folgenden Konsequenzen kommen:

- Verhängung von Bußgeldern oder Einleitung rechtlicher Schritte.
- Möglicher Ausschluss aus dem IHK-Register.

Um mögliche Nachteile zu vermeiden, empfehlen wir Ihnen, die Aktualisierung zeitnah vorzunehmen.

Unternehmensdaten jetzt aktualisieren

Vielen Dank für Ihre Kooperation. Bei Rückfragen steht Ihnen unser Kundenservice selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen,
Ihre Industrie- und Handelskammer (IHK)

https://www.ihk-muenchen.de/abzocke/

Was tun?:

Offensichtliche Spammails, die SPF und DKIM-Test bestehen: Missbrauch einer Internet-Domain!

„Abuse Contact“ finden: Rechtswidrigen oder missbräuchliche Nutzung einer Domain melden
Cyberangreifer wird Ressource entzogen - andere potenzielle Opfer besser geschützt.

E-Rechnungen per E-Mail: Spam, Betrug oder echt?

E-Mail mit PDF-(E-)Rechnung: Was tun?

- **Technischer Check** der E-Mail:

  SPF, DKIM, DMARC? Spam, Schadsoftware etc.?

  IHK: >90% aller Mails werden als Spam ausgefiltert

- **Inhalt prüfen**, besonders die IBAN → neue IBAN: verdächtig

  E-Rechnung XML anzeigen: https://quba-viewer.org

- Im Zweifelsfall: **Rückfragen** beim Rechnungssteller

E-Rechnungen per E-Mail: Spam, Betrug oder echt?

Jemand beschwert sich: Sie haben eine E-Rechnung gestellt, wissen davon nichts!

- **Cyberkriminelle haben in Ihrem Namen E-Rechnungen verschickt**

  Mit Ihrer Mailadresse? → SPF, DKIM, DMARC?

  „Nur“ mit Ihrem Namen → Kommunikation

- Maßnahmen gegen den Versand gefälschter Rechnungen in Ihrem Namen
- Schutzmechanismen gegen betrügerische E-Rechnungen

Notfallmaßnahmen: Was tun bei Betrugsfällen? Wer hilft?

Sie haben eine gefälschte (E-)Rechnung bezahlt?

- **Sofortmaßnahmen:**
  - Bank kontaktieren: Rückruf der Überweisung möglich?
  - Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Bayern:
    089/1212-3300 oder 110
    https://formularserver.bayern.de/intelliform/forms/rzsued/blka/blka/zac_checkliste/index
  - Betroffene informieren, z. B. tatsächlichen Geschäftspartner
  - IT-Abteilung oder IT-Dienstleister einschalten: Phishing-Angriff, Mail-Hack...?

Notfallmaßnahmen: Was tun bei Betrugsfällen? Wer hilft?

Sie haben eine gefälschte (E-)Rechnung bezahlt?

- **Weitere Schritte: Schadensbegrenzung, Prävention**
  - Geschäftsabläufe prüfen: Freigabe der Rechnung? Kontrollmechanismen lückenhaft? Interne Prozesse (z. B. Vier-Augen-Prinzip) überdenken und optimieren.
  - IT-Sicherheit stärken: SPF, DKIM und DMARC…
  - E-Mail-Sicherheitstools einsetzen
  - Mitarbeiterschulungen zu Phishing und Fake-Invoices durchführen
  - Mögliche Meldepflicht prüfen: IT-Sicherheitsgesetz? DSGVO? NIS2?

E-Mail: Absicherung verbessern

- Maßnahmen gegen den Versand gefälschter Rechnungen in Ihrem Namen
- Schutzmechanismen gegen betrügerische E-Rechnungen

E-Mail: Absicherung verbessern

- Tino Hager

Zusammenfassung – das Wichtigste im Überblick

- Eigene Domains, eigener E-Mailversand: SPF, DKIM, DMARC konfigurieren
- Empfangene E-Mails: Antispam- und Anti-Schadsoftware, auf SPF, DKIM… prüften und ggf. ausfiltern
- Kommunizieren Sie: Mit Dienstleistern, mit Rechnungsstellern, mit Rechnungsempfängern – ggf. telefonisch
- E-Rechnungen: XML-Daten entscheidend → Check per E-Rechnungsviewer wie z. B. Quba
- **Prüfen Sie besonders die Bankverbindung unbedingt sehr genau!**

Ziel des Webinars

Nach dem Webinar wissen Sie…

- …was eine E-Rechnung ist → **XML oder PDF Datei**
- …welche Transportmöglichkeiten es für E-Rechnungen gibt → **E-Mail, Schnittstellen, Portale**
- …warum man (E-)Rechnungen (per E-Mail) besonders genau prüfen sollte

  → **Rechnungen (fast) jeder Art sind leider fälschbar**
- …was man sofort tun kann um sein eigene E-Mailsicherheit zu verbessern

  → **SPF, DKIM, DMARC, AntiSpam, gesunder Menschenverstand**
- …wie man sich auf IT-Notfälle vorbereiten kann

  → **Kommunizieren (Bank, Polizei, Betroffene..), Prozesse & Technik verbessern**

IHK-NEWSLETTER BLEIBEN SIE INFORMIERT!