Essential Guide to E-Mail Security

Susan Rösner

Information Security Officer central services - Datacenter –

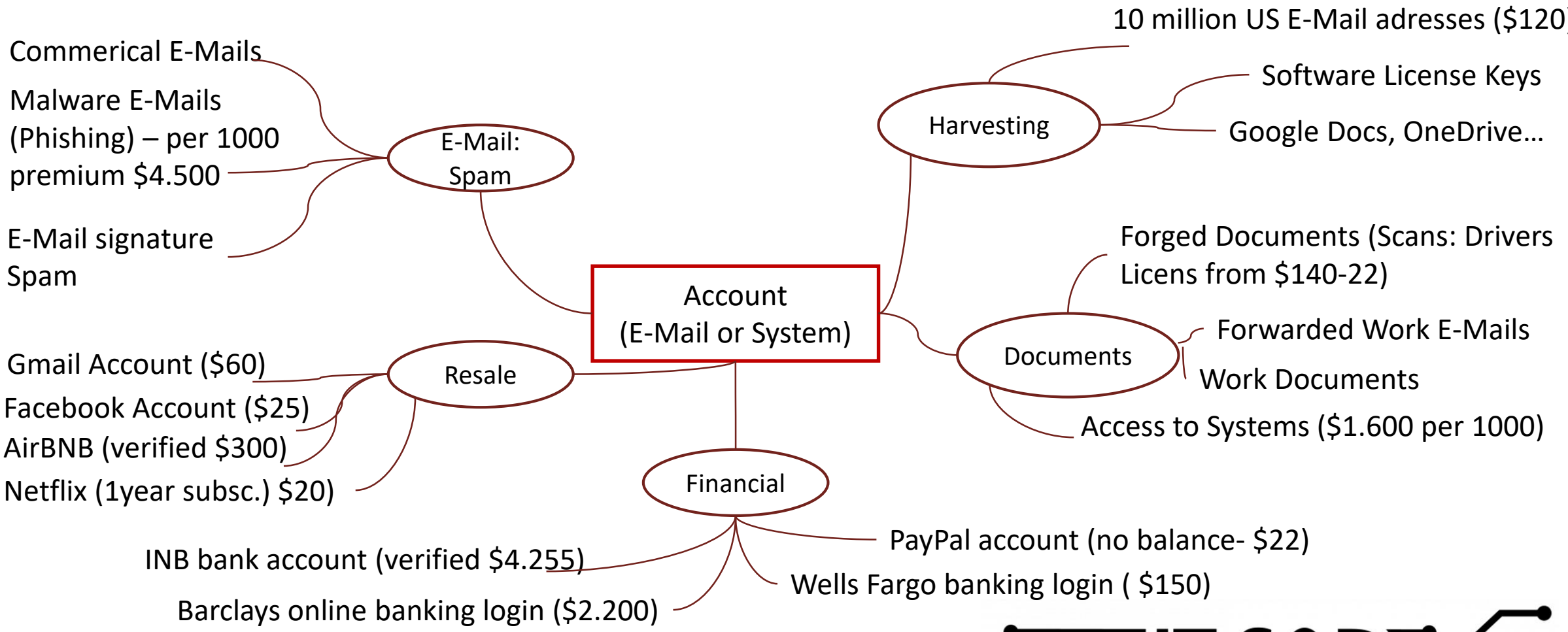
University Hildesheim

November, 13th 2024

How many accounts are connected to your E-Mail account?

IT-SAD
IT Security Awareness Days

E-Mail Security



Source: https://www.privacyaffairs.com/
Source: https://krebsonsecurity.com

IT-SAD
IT Security Awareness Days

Essential Guide to E-Mail Security

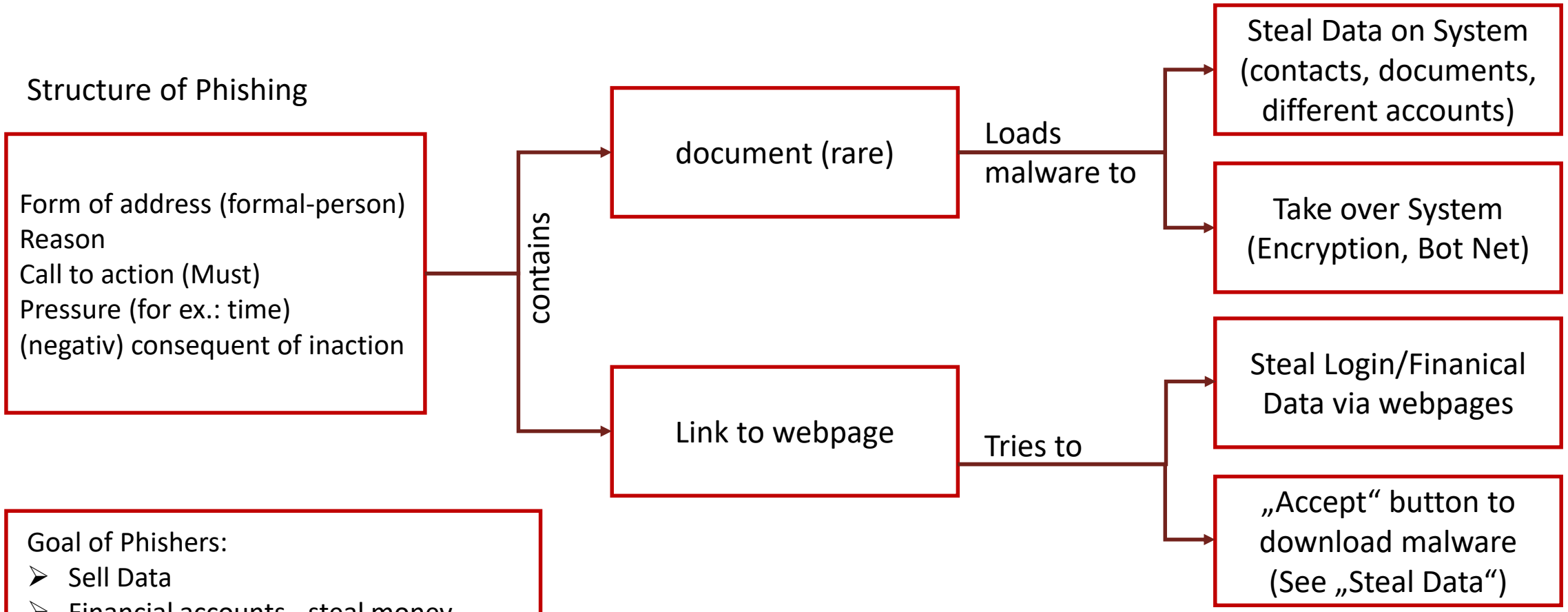
Agenda

Dos and don‘ts of information security

+ Definition of Phishing
+ Methodes of Phishers
+ Protection against Phishing

Definition of Phishing (Password + Fishing)

Structure of Phishing



Goal of Phishers:

- Sell Data
- Financial accounts - steal money
- Attack others based on your data
- Reputational damage

IT-SAD
IT Security Awareness Days

Essential Guide to E-Mail Security

Agenda

+ Definition of Phishing
+ Methodes of Phishers
+ Protection against Phishing

Methodes of Phishing (Password + Fishing)

- Topics to entice you:
  - current news
  - university project
  - Quotation from previous E-Mail
- Use human nature against us
  - Respect of authority or trusted people (Superior, government agency, friends)
  - Pressure
    - Time: CEO Fraud (financial fraud)
    - Anxiety/fear: Account closed
    - Greed: first 50 replies win a price or discount
  - Automatic action like Button in E-Mail (highlighted: underline or frame)
  - Curiosity: list of Earnings of celebrity/co-worker

IT-SAD
IT Security Awareness Days

Example

Signs of Phishing mail: pressure=time | mouse over of link showed non-UHI domain | e-mail domain non-UHI domain

Betreff:Überprüfen Sie Ihr Konto
Datum: Mon, 28 Oct 2024 01:50:22 -0400
Von: Universität Hildesheim Webmail <nityanand@nitk.ac.in>

Universität Hildesheim Webmail

Ablauf der E-Mail-Adresse

Lieber Benutzer,

Ihr Kontopasswort läuft heute, am 28.Oktober 2024, ab. Um Ihr Postfach weiterhin nutzen zu können, müssen Sie unten Ihr Passwort bes

https://rolo-etherea.hunterdouglas.com.br/s2/s2.html
Klicken oder tippen Sie, um dem Link zu folgen.

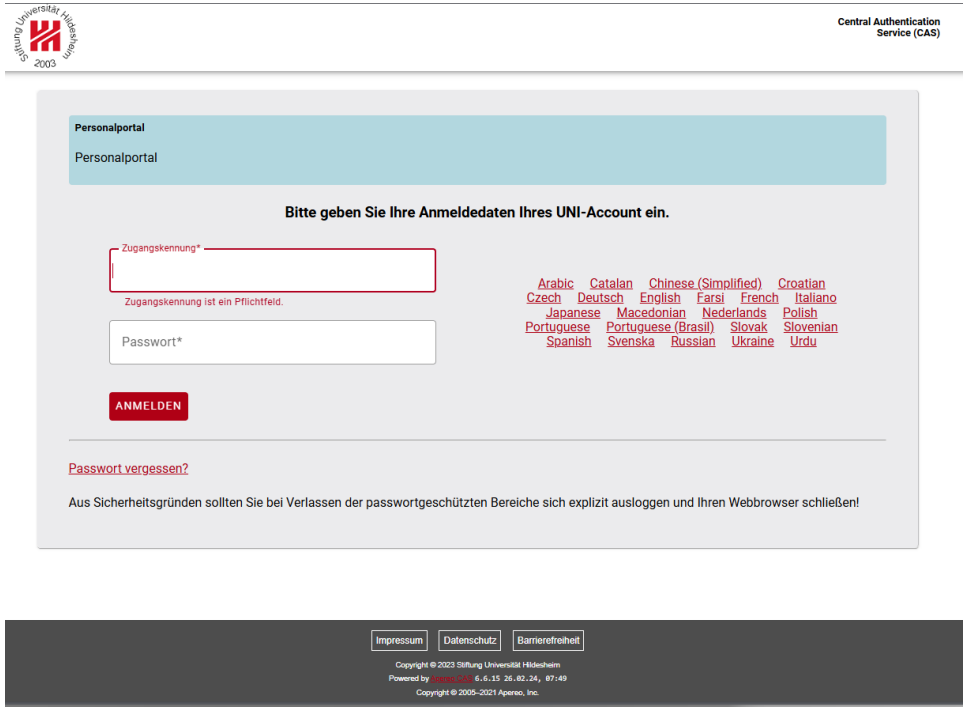
ÜBERPRÜFEN SIE IHR KONTO

IT-SUPPORT

Universität Hildesheim Webmail

--
-- Mail through NITK (http://www.nitk.ac.in/) Email Gateway (mx1.nitk.ac.in) --

If link was clicked: transfer to 1:1 copy of UHI Login page – only URL differed



IT-SAD
IT Security Awareness Days

Example

-------- Weitergeleitete Nachricht --------
Betreff: Rechnung 22400799 als PDF
Datum: Tue, 22 Oct 2024 05:07:08 +0000
Von: Aidin Yousefi <no-reply@gandrolizdas.com>
An: [redacted]@uni-hildesheim.de>

Sehr geehrte Damen und Herren,

anbei erhalten Sie unsere Rechnung Nr. 22400799 vom 30.09.2024 als PDF-Datei.

Können wir sonst noch etwas für Sie tun? Sprechen Sie uns gerne an.

Viele Grüße

---

i.A. Aidin Yousefi
Nauenweg 135
47798 Krefeld

Engel Haustechnik GmbH & Co. KG
E-Mail: a.yousefi@engel-haustechnik.de
Web: www.engel-haustechnik.de
Telefon: 02151 76 76 457

Sitz: Krefeld - Registergericht: Amtsgericht Krefeld, HRA7238 |Geschäftsführer: Sebastian Engel

Signs of Phishing mail: e-mail domain different to correct one (in signature) | send to user that has nothing to do with billing -> in this case an attachment (invoice) contained malicious code

IT-SAD
IT Security Awareness Days

Essential Guide to E-Mail Security

Agenda

+ Definition of Phishing
+ Methodes of Phishers
+ Protection against Phishing

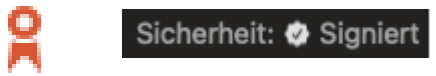
Understanding E-Mail

- E-Mail is like sending a postcard
  - it is not secure – do not automatically trust its content and
  - you cannot be sure of sender (unless signed)
  - most attributes can be faked / hidden (sender, links, …)

IT-SAD
IT Security Awareness Days

Understanding E-Mail

- Sender address is always trustworthy (?)
  - NO – unless E-Mail is signed
  - Example of Signed E-Mails (depend on your e-mail client):



(please asked your technical support for options to use e-mail signatures)

  - Example of misleading sender:
    - „Susan Roesner“
    - „Susan Roesner“ susan.roesner74@gmail.com
    - „Susan Roesner – roesner@uni-hildesheim.de“ roesner@googlebooks.com
    - „Susan Roesner“ roesner@uni-hildeshiem.de

IT-SAD
IT Security Awareness Days

Understanding E-Mail

- check E-Mail header or ask your HelpDesk if suspicious

(under „received“ – in reverse order – you will see from which e-mail server the mail was send

here: e-mail from DELL – so the first e-mail server should be from DELL

here: at the bottom: DKIM Signature – this is new option to ensure that E-Mail server is truly from DELL – therefor mail can be trusted that origin is DELL)

- Link to further information:

https://www.uni-hildesheim.de/en/rz/it-dienste/it-sicherheit/sichere-e-mail/

```
Return-Path: <prvs=10460c3fbe=cce.legal.bounceback@dell.com>
Delivered-To: roesner@uni-hildesheim.de
Received: from mailf1.rz.uni-hildesheim.de ([127.0.0.1])
        (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits))
        by mailb2.rz.uni-hildesheim.de with LMTPS
        id kCLiM+luM2cfCCoAFV0O9Q:P1
        (envelope-from <prvs=10460c3fbe=cce.legal.bounceback@dell.com>)
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 16:06:17 +0100
Received: from mailf1.rz.uni-hildesheim.de ([127.0.0.1])
        by mailf1.rz.uni-hildesheim.de with LMTP
        id kCLiM+luM2cfCCoAFV0O9Q
        (envelope-from <prvs=10460c3fbe=cce.legal.bounceback@dell.com>)
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 16:06:17 +0100
Received: from robin.uni-hildesheim.de (robin.uni-hildesheim.de [147.172.16.6])
        (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
         key-exchange ECDHE (P-256) server-signature RSA-PSS (2048 bits) server-digest SHA256)
        (No client certificate requested)
        by mailf1.rz.uni-hildesheim.de (Postfix) with ESMTPS id 4XnqVx5d0TzDqCr
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 16:06:17 +0100 (CET)
Received: from mx0a-00154904.pphosted.com ([148.163.133.20])
        by robin.uni-hildesheim.de with esmtps  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        (Exim 4.97)
        (envelope-from <prvs=10460c3fbe=cce.legal.bounceback@dell.com>)
        id 1tAsT8-00000008k8O-1kK1
        for roesner@uni-hildesheim.de;
        Tue, 12 Nov 2024 15:06:17 +0000
Received: from pps.filterd (m0170391.ppops.net [127.0.0.1])
        by mx0a-00154904.pphosted.com (8.18.1.2/8.18.1.2) with ESMTP id 4ACCcYaH024754
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 10:06:12 -0500
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=dell.com; h=
        content-type:date:from:message-id:mime-version:subject:to; s=
        smtpout1; bh=U5J0dUCVaBCH1e91aQX1JwVsHTDpRID1hNRsIfpYiwQ=; b=CDs
        dqYqeNOMZPjHHoHi7mQeNYNBQFkVASEIfJiaLT9zxaoubk8Gt+SVv9HuzVo/H+y3
        TWHakYixQkFcv3XtkLw/YxEeInkGvGVnFzFUBr00Ok1NkpPP6bvweKspiuFmETN9
        ia7fyL+q742lTfHG2OkidBvK2rAst0FVJsrW7Lo6fkc3I/eiYkSJVk2xkn+cBiyi
        QpbILsno6S9sHJWGc1iNYivQxZVQsx9dnFdwuYCrpttAek4n5Uagu/MRM3vjadl3
        QKNtQDvKeNiBiDpzx6FUF9Jb9dR+OUBZg+2k4lM3rxZLgXeLIe4zgjzWmfOz9WWo
        KJx100a6Z4BcVkoGOpQ==
Received: from mx0b-00154901.pphosted.com (mx0b-00154901.pphosted.com [67.231.157.37])
        by mx0a-00154904.pphosted.com (PPS) with ESMTPS id 42v7721hut-1
        (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NOT)
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 10:05:13 -0500 (EST)
Received: from pps.filterd (m0393468.ppops.net [127.0.0.1])
        by mx0a-00154901.pphosted.com (8.18.1.2/8.18.1.2) with ESMTP id 4ACEsMnQ025332
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 10:04:11 -0500
Received: from esapsmtplv08.us.dell.com (esapsmtplv08.us.dell.com [143.166.203.145])
        by mx0a-00154901.pphosted.com (PPS) with ESMTPS id 42t3p4bgwu-1
        (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=OK)
        for <roesner@uni-hildesheim.de>; Tue, 12 Nov 2024 10:04:02 -0500 (EST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=dell.com; i=@dell.com; q=dns/txt; s=smtpdev1;
  t=1731423841; x=1762959841;
  h=date:from:to:message-id:subject:mime-version;
  bh=U5J0dUCVaBCH1e91aQX1JwVsHTDpRID1hNRsIfpYiwQ=;
  b=SyxIE/BAXgFpwvKYX/8ZzbQG5FEXcu7/wZUNh6tsWA1S2MUeZ53MAp1c
```

Understanding Links

- https://uni-hildesheim.de/rz

Protocoll = https means secure

Domain Name = name + (uni-hildesheim | amazon | nytimes…) + top Level domain (de | com | org | shop…)

Path to information on a specific webpage – this is not part of domain name
!!! domain name always ends at **last** „.“ + top level domain like „.de“ or „.com“ !!!

- human nature used against us through pattern
  - https://paypa1.de → substitut l through 1
  - https://vveather.com → substitut W trough V V
  - https://arnazon.com → substitut m through ar
  - https://uni-hildesheim.de.rz.de → remember domain level structure | someone registered domain not belonging to UHI
    (remember domain name ends at **last** „.“)

IT-SAD
IT Security Awareness Days

How to secure/check an E-Mail

- configure your mail client: use TXT instead of HTML (Link in clear text, hidden formation not working…)
- does E-Mail follow typical phishing format (pressure, negativ consequent, link or attachment)
  - I do not mean: 3 week deadline
  - I do not mean: link when requested, or known project…)
- ask yourself:
  - is the topic relevant to you (are you working on referenced project, do you expect a package, are you custommer of service…)
  - is the e-mail sender valid

IT-SAD
IT Security Awareness Days

How to secure/check an E-Mail

- if suspicious do
  - check link (mouse over)
  - if you are not sure of link:
    - check certificate of webpage
    - never click on link – enter URL yourself or search for correct URL (using search engine like duckduckgo | bing | google….)
    - search original Webpage for reverenced project (news)
  - NEVER reply or call back – check for correct telephone number or on official webpage for contact details
    - if it is spam or phishing attack: answering e-mail = your e-mail is verified to belong to a human/is active → your e-mail adress is now valuable and will be sold

IT-SAD
IT Security Awareness Days

You clicked on Link/document – what now?

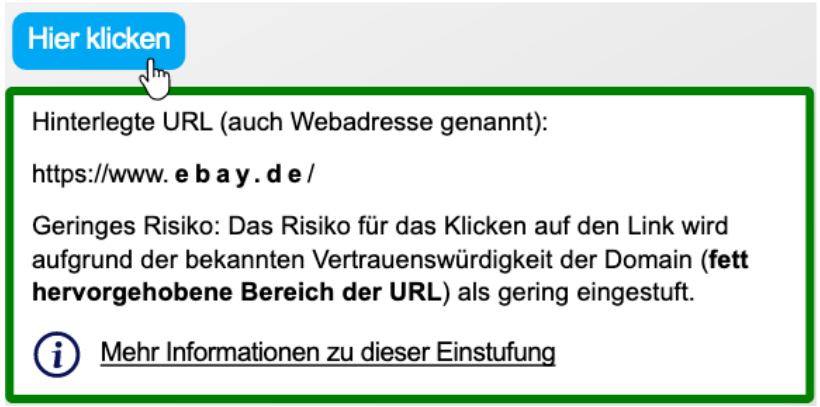
- Don‘t panic – it happend
- Please: do not ignore
- Do not turn off system – disconnect at once (cable or WLAN)
- Call IT-Service Desk – or if dedicated contact like e-mail phone or contact Information Security Officer office

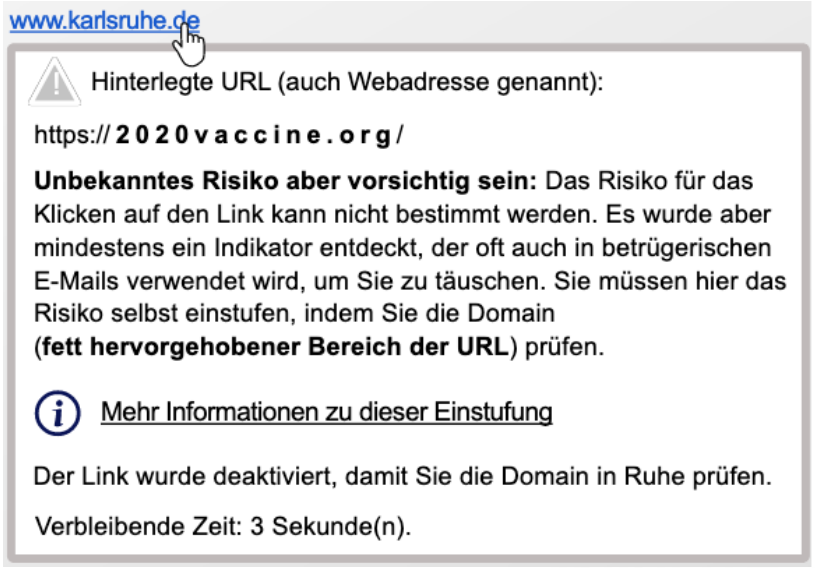
- if it happens with your private E-Mail account:
  - change credentials (from different system)
  - use c‘t emergency toolkit or similar (get it bevor something happens to have it available) to scan your system
  - in case credit/debit cards: call 116 116

IT-SAD
IT Security Awareness Days

How to secure/check an E-Mail

- Browser (firefox and Chrome) and Thunderbird Add-On to recognize Phishing E-Mails
- https://secuso.aifb.kit.edu/TORPEDO.php

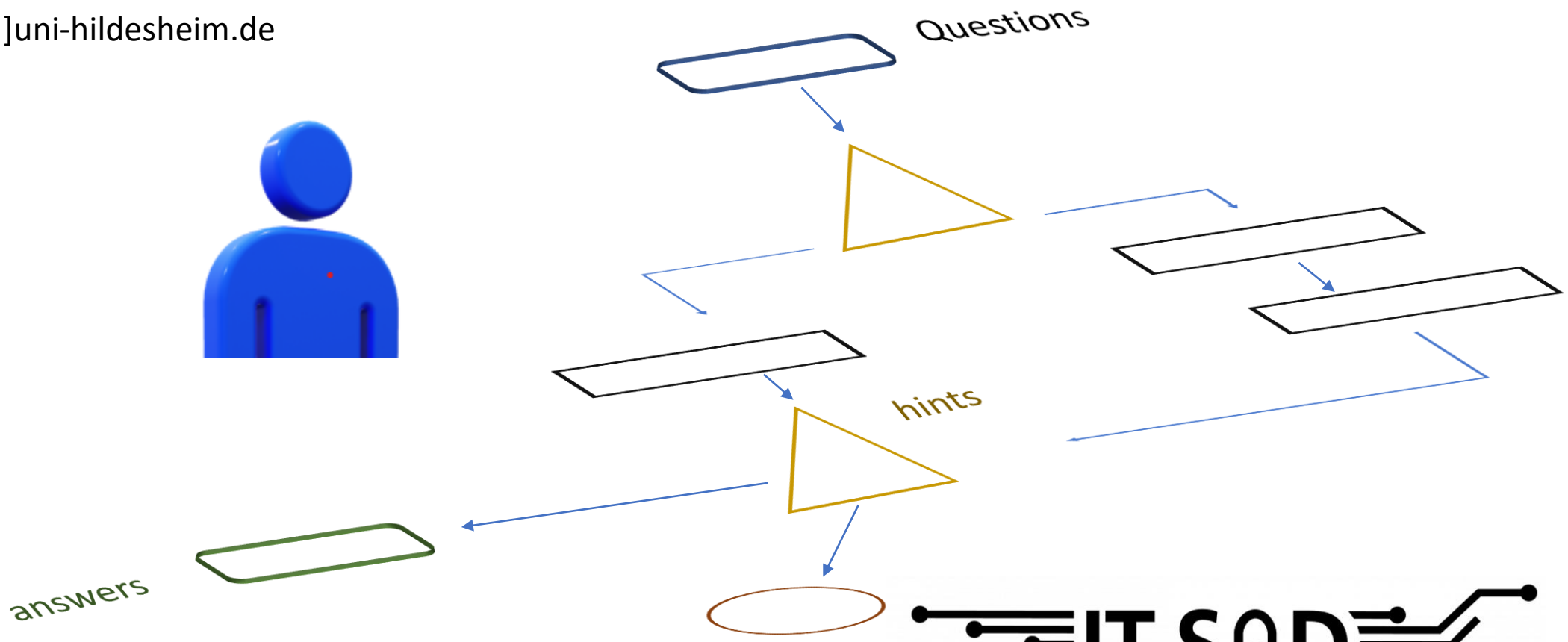




IT-SAD
IT Security Awareness Days

Fragen

Susan Roesner
it-sicherheit[@]uni-hildesheim.de



IT-SAD
IT Security Awareness Days