Phishers Fritze phisht…

Neues vom Anglerladen

Inhalt

- **Bei mir gibt‘s doch nichts zu holen**
- **Phishing & Malware**
- **Zertifikate & digitale Signaturen**
- **Geräte-Sicherheit**
- **Updates & Backups**

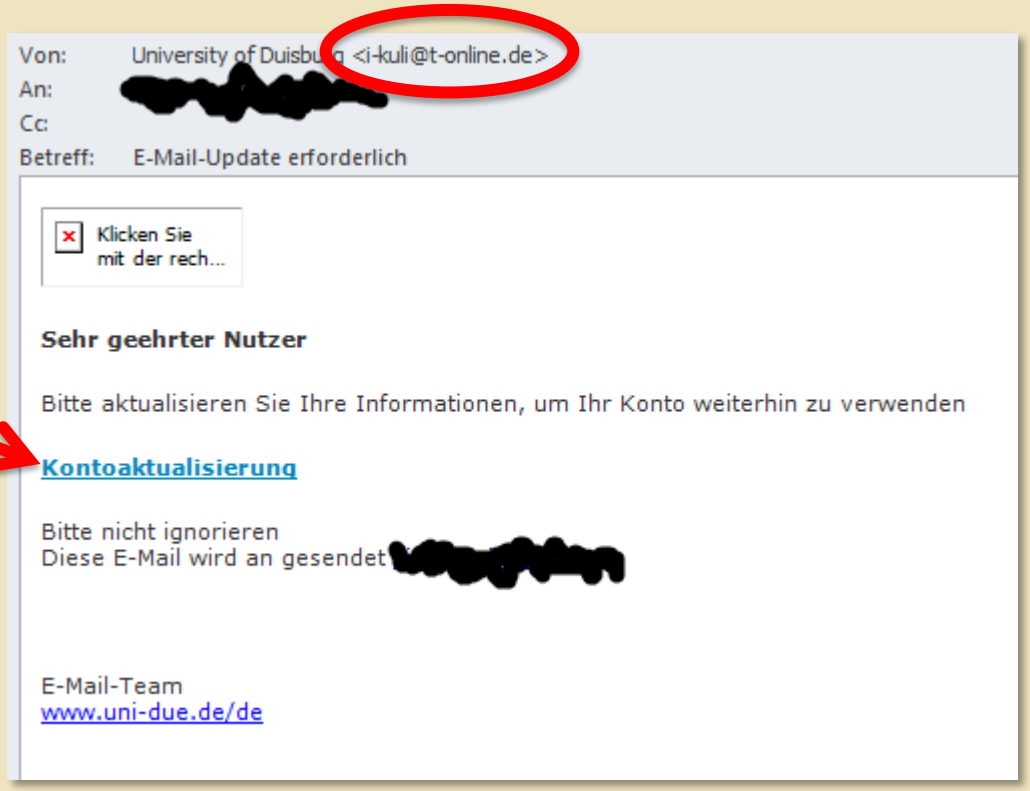
Bei mir gibt‘s doch nichts zu holen

- **Login-Informationen**
  → Informationssammlung, Spam-Versand
- **Online-Banking**
  → Unautorisierte Abbuchungen, Kreditkartendaten
- **Persönliche Daten**
  → Überzeugendere Spam-Generierung
- **Kontakte**
  → Weiterverkauf der Datensätze
- **Rechenleistung**
  → Mining von Cryptowährung
- **Proxy-Dienste**
  → Verschleiern der Angreifer-Aktivitäten

Phishing

- **Sehr einfach gemachte Phishing-Mail**

Link zu gefälschter Login-Seite



Phishing

- **Ansicht als Nur-Text**

Von: University of Duisburg <i-kuli@t-online.de>
An: [redacted]
Cc:
Betreff: E-Mail-Update erforderlich

<https://webmailer.uni-duisburg-essen.de/skins/uni-due/images/roundcube_logo.png>

Sehr geehrter Nutzer

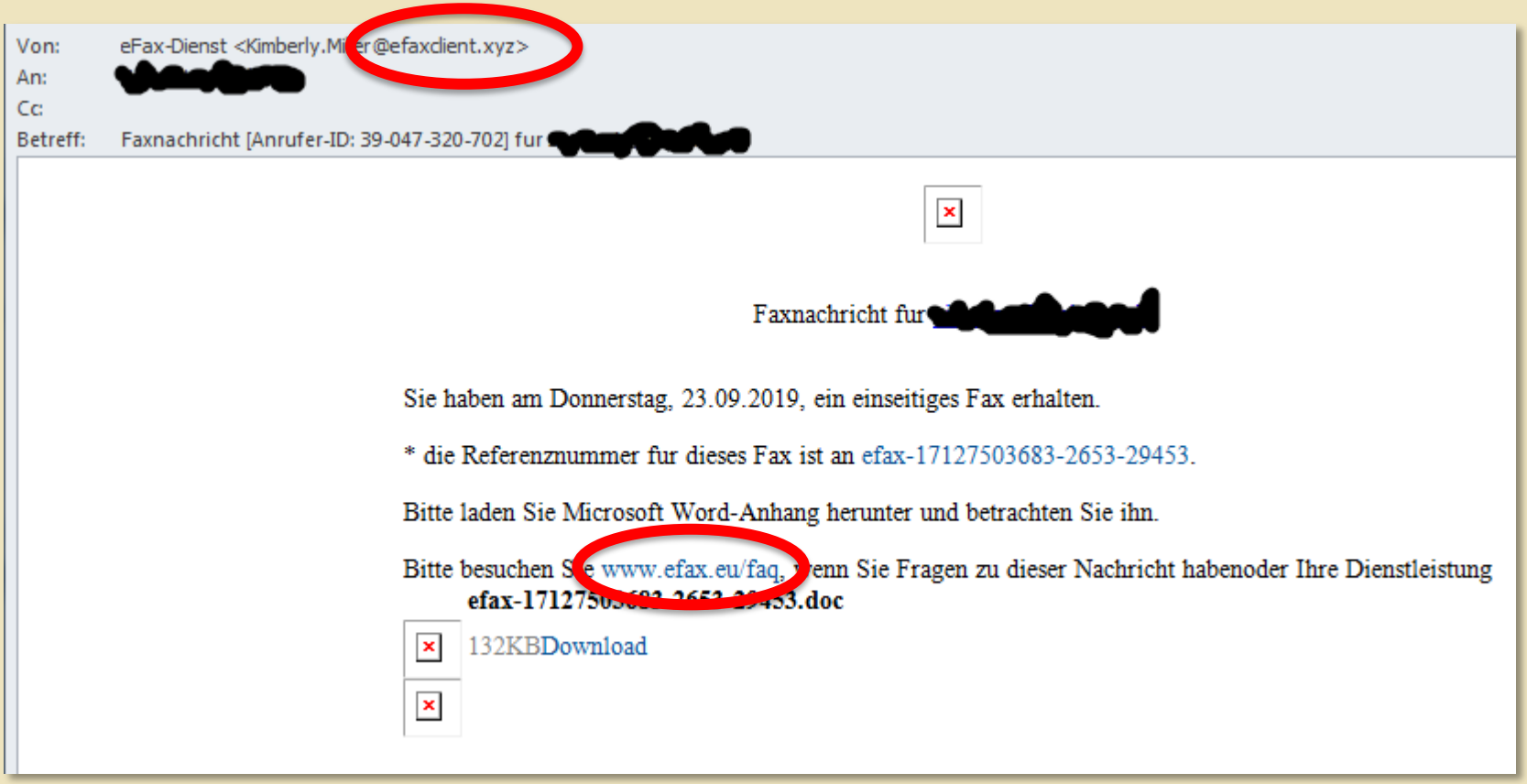
Bitte aktualisieren Sie Ihre Informationen, um Ihr Konto weiterhin zu verwenden

Kontoaktualisierung <http://wholesalepresentationfolder.com/roundcube/roundcube/index.php?_user=[redacted]

Bitte nicht ignorieren
Diese E-Mail wird an gesendet [redacted]

E-Mail-Team
www.uni-due.de/de

eFax



Von: eFax-Dienst <Kimberly.M[redacted]@efaxclient.xyz>
An: [redacted]
Cc:
Betreff: Faxnachricht [Anrufer-ID: 39-047-320-702] fur [redacted]

Faxnachricht fur [redacted]

Sie haben am Donnerstag, 23.09.2019, ein einseitiges Fax erhalten.

* die Referenznummer fur dieses Fax ist an efax-17127503683-2653-29453.

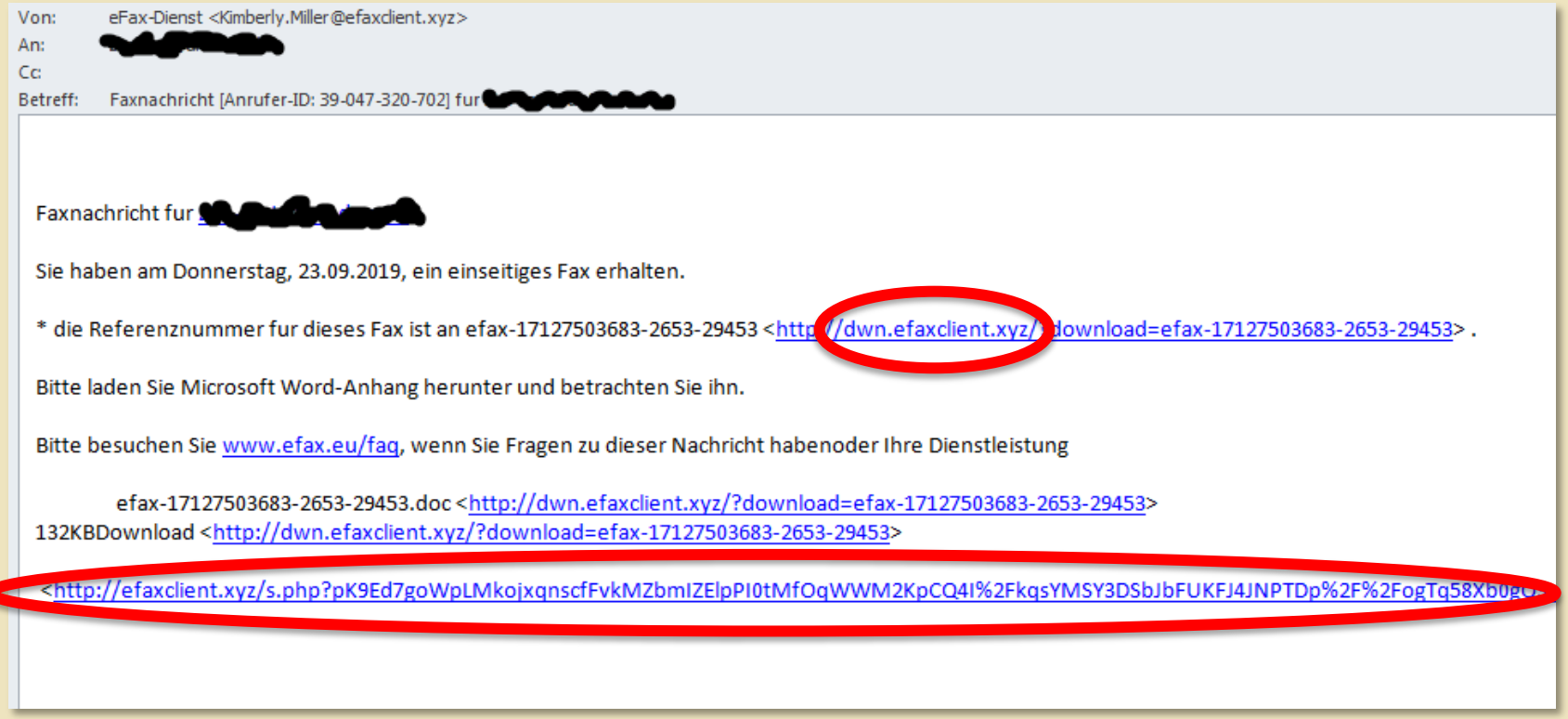
Bitte laden Sie Microsoft Word-Anhang herunter und betrachten Sie ihn.

Bitte besuchen S[redacted] www.efax.eu/faq, [redacted]enn Sie Fragen zu dieser Nachricht habenoder Ihre Dienstleistung

efax-1712750[redacted]453.doc

132KBDownload

- **Ansicht als Nur-Text**



Von: eFax-Dienst <Kimberly.Miller@efaxclient.xyz>
An: [redacted]
Cc:
Betreff: Faxnachricht [Anrufer-ID: 39-047-320-702] fur [redacted]

Faxnachricht fur [redacted]

Sie haben am Donnerstag, 23.09.2019, ein einseitiges Fax erhalten.

* die Referenznummer fur dieses Fax ist an efax-17127503683-2653-29453 <http://dwn.efaxclient.xyz/?download=efax-17127503683-2653-29453> .

Bitte laden Sie Microsoft Word-Anhang herunter und betrachten Sie ihn.

Bitte besuchen Sie www.efax.eu/faq, wenn Sie Fragen zu dieser Nachricht habenoder Ihre Dienstleistung

efax-17127503683-2653-29453.doc <http://dwn.efaxclient.xyz/?download=efax-17127503683-2653-29453>
132KBDownload <http://dwn.efaxclient.xyz/?download=efax-17127503683-2653-29453>

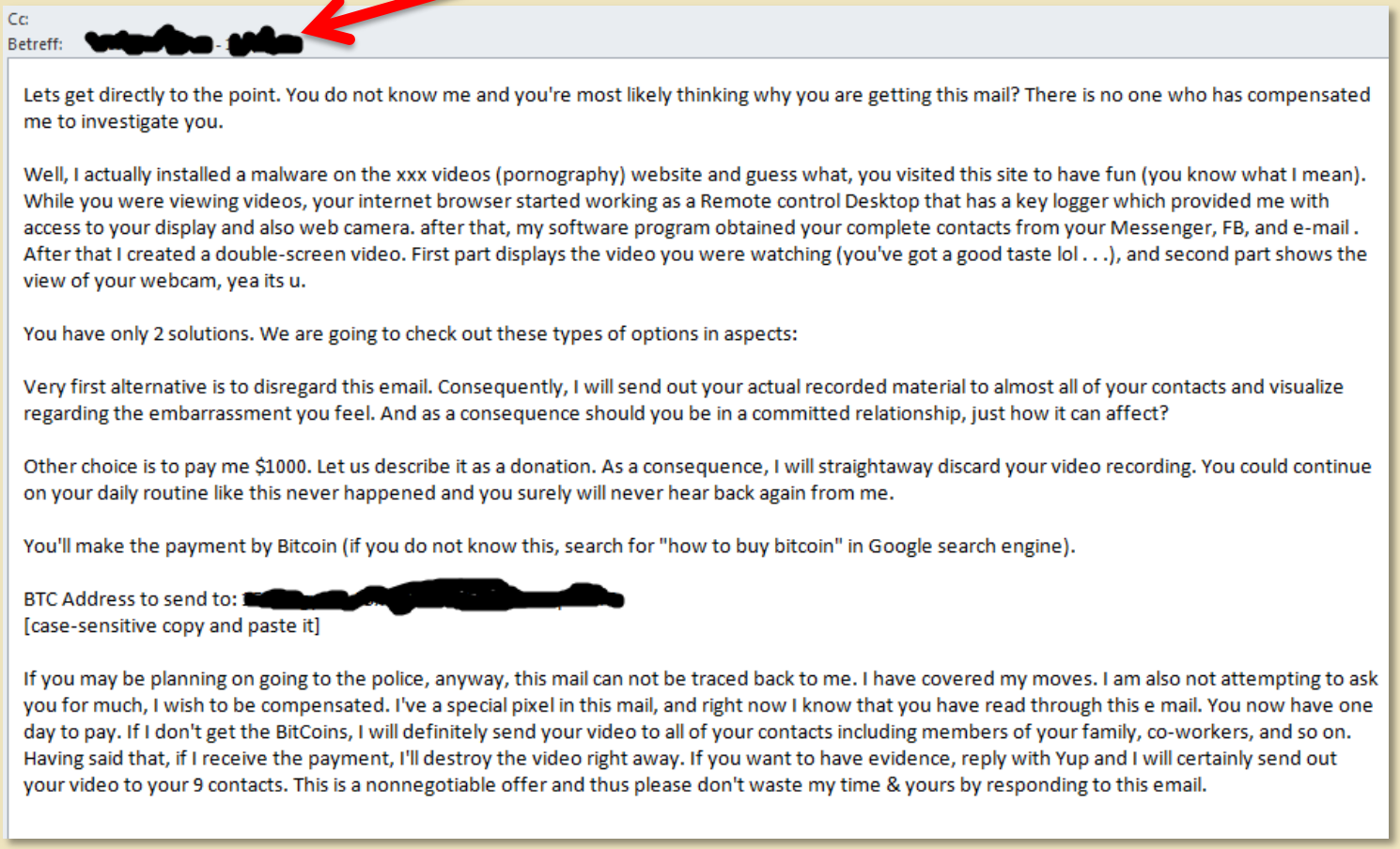
<http://efaxclient.xyz/s.php?pK9Ed7goWpLMkojxqnscfFvkMZbmIZElpPI0tMfOqWWM2KpCQ4I%2FkqsYMSY3DSbJbFUKFJ4JNPTDp%2F%2FogTq58Xb0gC>

Whois-Abfrage efaxclient.xyz

```
Domain Name: EFAXCLIENT.XYZ
Registry Domain ID: D130557456-CNIC
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: https://publicdomainregistry.com
Updated Date: 2019-09-22T11:00:46.0Z
Creation Date: 2019-09-22T11:00:45.0Z
Registry Expiry Date: 2020-09-22T23:59:59.0Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: N/A
Registrant State/Province: Sverdlovskaya oblast
Registrant Country: RU
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for
information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for
information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: DNS4.REGWAY.COM
Name Server: DNS3.REGWAY.COM
Name Server: DNS2.REGWAY.COM
Name Server: DNS1.REGWAY.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for
information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Erpressung

Echtes Passwort des Nutzers



Cc:
Betreff: [redacted]

Lets get directly to the point. You do not know me and you're most likely thinking why you are getting this mail? There is no one who has compensated me to investigate you.

Well, I actually installed a malware on the xxx videos (pornography) website and guess what, you visited this site to have fun (you know what I mean). While you were viewing videos, your internet browser started working as a Remote control Desktop that has a key logger which provided me with access to your display and also web camera. after that, my software program obtained your complete contacts from your Messenger, FB, and e-mail . After that I created a double-screen video. First part displays the video you were watching (you've got a good taste lol . . .), and second part shows the view of your webcam, yea its u.

You have only 2 solutions. We are going to check out these types of options in aspects:

Very first alternative is to disregard this email. Consequently, I will send out your actual recorded material to almost all of your contacts and visualize regarding the embarrassment you feel. And as a consequence should you be in a committed relationship, just how it can affect?

Other choice is to pay me $1000. Let us describe it as a donation. As a consequence, I will straightaway discard your video recording. You could continue on your daily routine like this never happened and you surely will never hear back again from me.

You'll make the payment by Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google search engine).

BTC Address to send to: [redacted]
[case-sensitive copy and paste it]

If you may be planning on going to the police, anyway, this mail can not be traced back to me. I have covered my moves. I am also not attempting to ask you for much, I wish to be compensated. I've a special pixel in this mail, and right now I know that you have read through this e mail. You now have one day to pay. If I don't get the BitCoins, I will definitely send your video to all of your contacts including members of your family, co-workers, and so on. Having said that, if I receive the payment, I'll destroy the video right away. If you want to have evidence, reply with Yup and I will certainly send out your video to your 9 contacts. This is a nonnegotiable offer and thus please don't waste my time & yours by responding to this email.

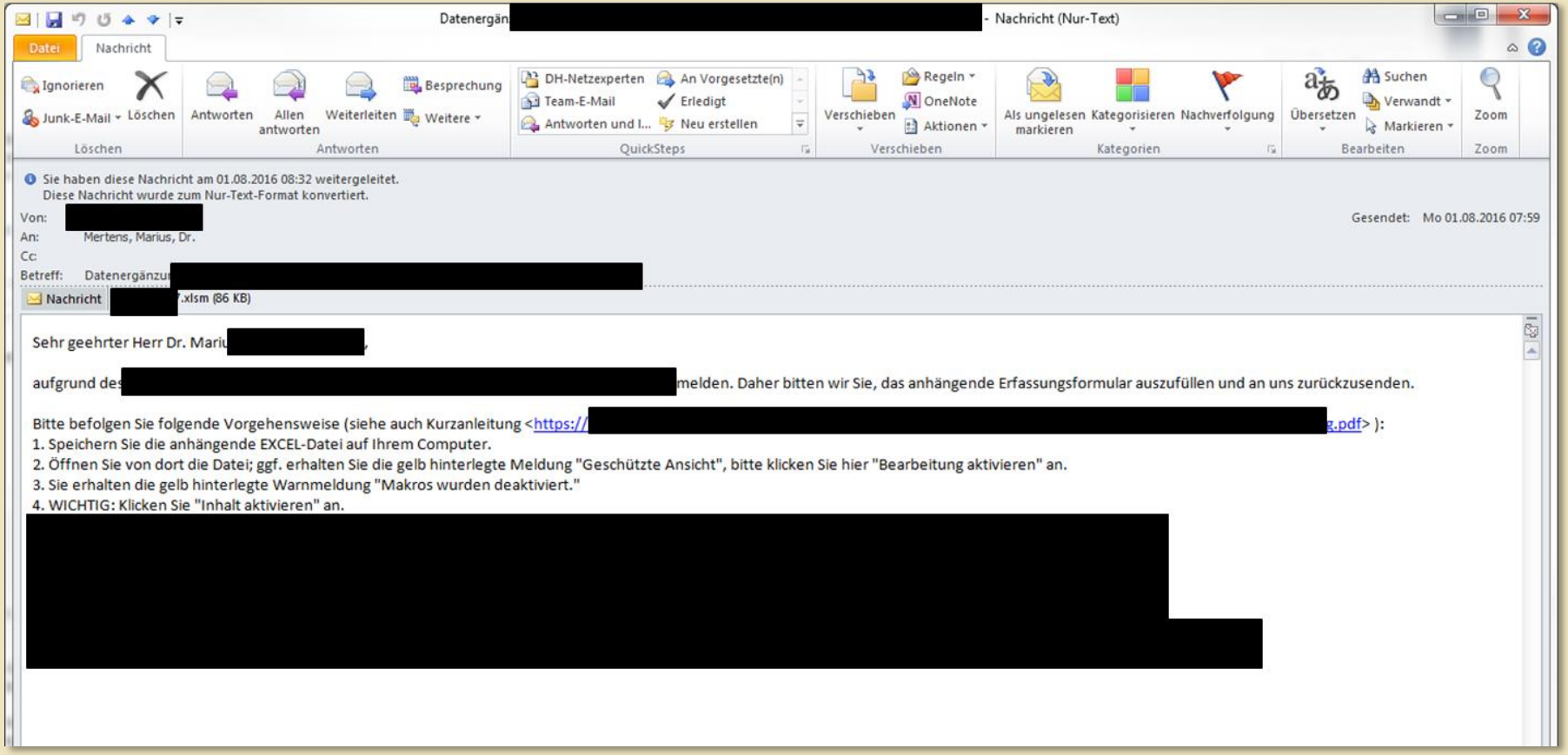
Collection #1 und Co

- **Quellen für Login-Daten**
  - Phishing
  - Datenabfluss bei großen Unternehmen
  - Malware
  - Bruteforce
- **Aggregation, Verkauf**
- **Anfang 2019: Veröffentlichung von Sammlungen mit 2,2 Milliarden Accounts**
- **Test auf Datenlecks**
  - https://haveibeenpwned.com/
  - https://sec.hpi.de/ilc/

Umgang mit Spam

- **Ziel des Angreifers: Opfer soll reagieren**
  - Etwas ausführen
  - Etwas herunterladen (und dann ausführen)
  - Etwas eingeben
- **Beim leisesten Verdacht: Besser nichts tun**
  - hotline.zim@uni-due.de fragen
- **Spammer wissen, wie legitime Mails aussehen**
  … und lernen ständig dazu
- **Viel offensichtlicher Spam**
  … aber immer wieder sehr gut gemachte Ausnahmen
- **Gefahr: Malware per Link. Statt öffentlichen Cloud-Speichern besser die hauseigenen Alternativen nutzen:**
  - Gigamove: https://www.uni-due.de/zim/services/gigamove.php
  - Sciebo: https://www.uni-due.de/zim/services/sciebo/
- **Sicherheitskultur: Lassen Sie Ihre Mails nicht wie Spam aussehen!**

Gefährlich oder harmlos?



Was ist Emotet?

- Bekannt seit 2014
- Eigentlich Banking-Trojaner
- Polymorph → Signaturbasierte Virenscanner versagen in der Regel
- Sandboxerkennung
- Modularer Aufbau
- Command & Control Server für Befehle, Updates, Payload
- Exfiltration von Kommunikationsdaten und Passwörtern
- Distributions-Framework: Mail, Remoteadmin, Kerberos Hijacking, PW-Bruteforce, Schwachstellen (EternalBlue etc.)
- Atombombe für die Hosentasche

Was ist Emotet?

- Bekannt seit 2014
- Eigentlich Banking-Trojaner
- Polymorph → Signaturba… Virenscanner ver…
- Sandboxerke…
- Modularer Aufb…
- Command & Control Se… hle, Updates, Payload
- Exfiltration von Kommuni… aten und Passwörtern
- Distributions-Framewo… Remoteadmin, Kerbero… V-Bruteforce, Schwachst… ue etc.)
- Atombombe für die Hosentasche

Emotet-Infektionsverlauf

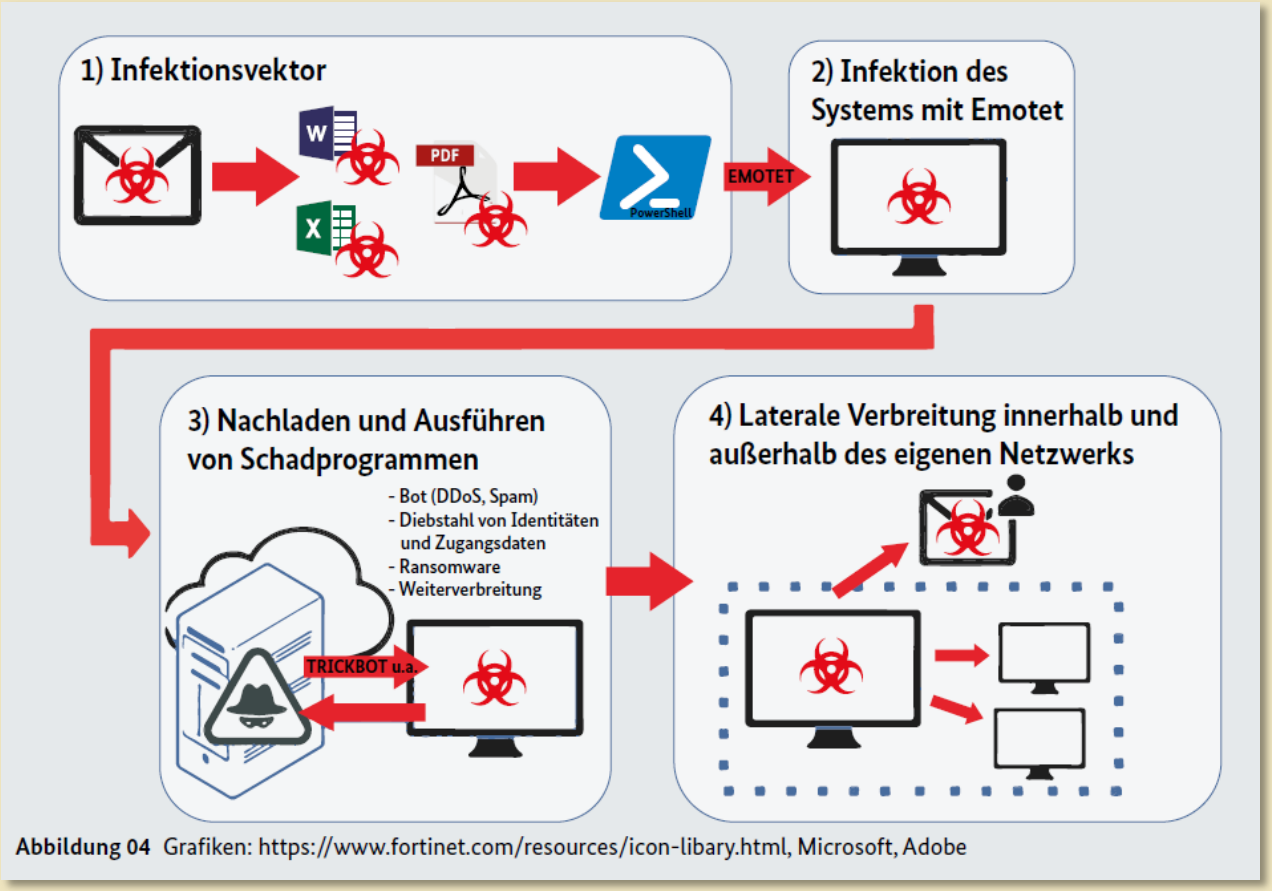


Abbildung 04 Grafiken: https://www.fortinet.com/resources/icon-libary.html, Microsoft, Adobe

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2019

Emotet an der UDE

≤2018: Diverse Phishing-Wellen, immer wieder .doc-Dateien mit Malware, immer wieder Opfer trotz vielfältiger Aufklärung, mal Emotet, mal Anderes

November 2018: Sperrung der Legacy-Office-Formate geplant

Anfang 2019: Vorstellung in den IT-Gremien

Mai 2019: Emotet-Angriff mit zuvor erbeuteten Daten und Malware im Mail-Anhang

Juni 2019: Rektoratsbeschluss: Sperrung der gefährlichen Anhänge. Signierte Informationsmail an alle Hochschulangehörigen

Juli 2019: Veraltete Office-Formate werden vom Mailserver abgewiesen

August 2019: Auch Cyberkriminelle machen Urlaub

September 2019: Emotet-Mails mit alten Inhalten und variierendem Schadcode-Container treffen ein → Tests auf Schutzmaßnahmen.
Erneuter Angriff mit Schadcode in .rtf-Dokumenten

Gegenmaßnahmen

> Eine restriktive Behandlung von Anhängen (Dateityp-Whitelist-Ansatz) verbunden mit einer restriktiven Content-Policy für Dokumente (indem z. B. Dokumente mit Makros oder Nachladefunktionalität oder Office-Nachladeanfragen am zentralen HTTP-Gateway gefiltert werden) könnte die meisten neuen Ansätze der Angreifer ins Leere laufen lassen.

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2019

> Dass nicht alle technisch ausgeklügelten Ansätze der Angreifer in der Praxis erfolgreich sind, zeigt sich an den passwortgeschützten ZIP-Dateien. Diese haben zwar die Perimeter-Antiviren-Lösungen leicht überwunden, scheinen aber an den Nutzern gescheitert zu sein, die nicht gewillt oder nicht in der Lage waren, Passwörter beim Öffnen des Anhangs einzugeben.

Müssen Nutzer mit einem Mausklick das ganze System lahmlegen können?
→ Nur signierte Makros erlauben per Gruppenrichtlinie

„Nach“ Emotet

- Vorgesetzte mit S-MIME-Zertifikat ausgestattet
  - Vorbildfunktion
  - Stark verbreitete S-MIME-Signatur unter den Mitarbeitern
- Crypto-Partys in den Abteilungen der Hochschulverwaltung
- Infomail durch RZ-Leiter an alle Hochschulangehörigen
  - Sperrung der Legacy-Office-Formate
  - Phishing-Warnung
  - Information über meldepflichtigen Datenschutzvorfall
- Sperrung der Legacy-Office-Formate (allerdings nicht sofort, sondern erst nach erneutem Gremien-Lauf per Rektoratsbeschluss)
- Verpflichtende Awareness-Schulung für alle Mitarbeiter
- **Nicht vergessen: Auch von mittlerweile bereinigten Rechnern wird die abgegriffene Kommunikation weiterhin für Angriffe verwendet!**
- **Gibt es weitere infizierte Rechner?**
- **Sind Administratorkennwörter kompromittiert?**

Lessons learned

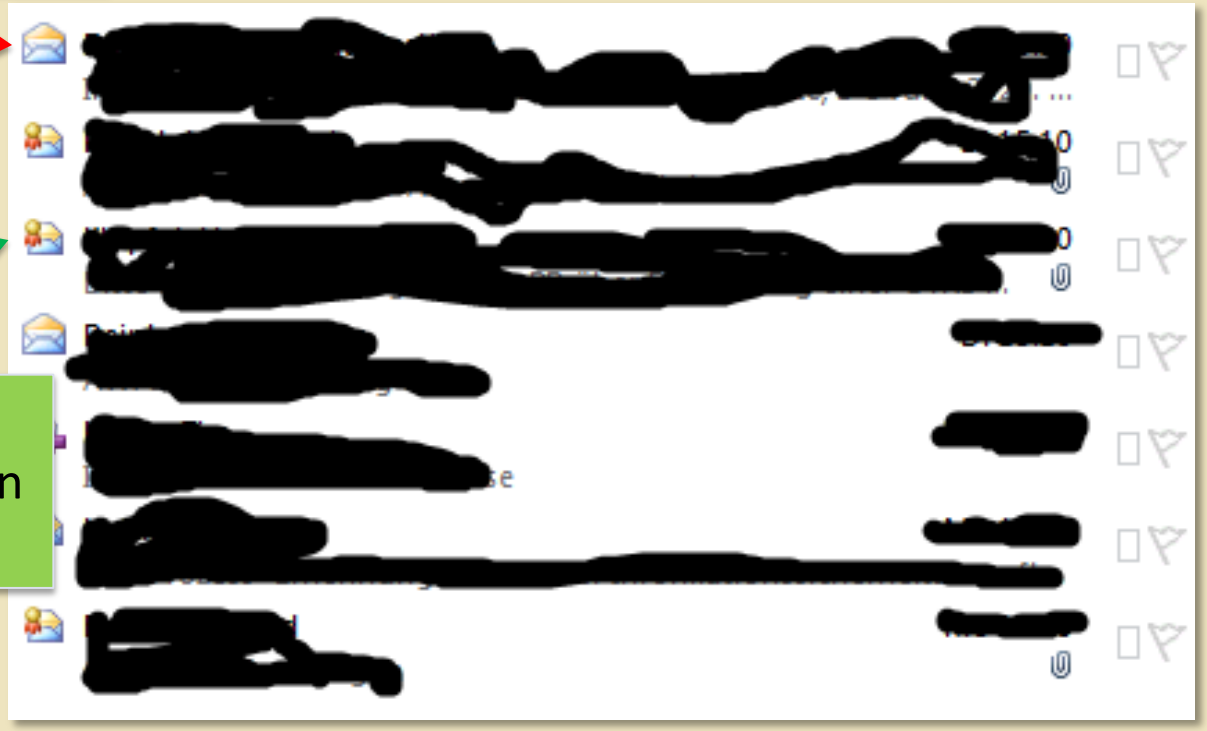
- **Trotz intensiver Information sind nicht alle Nutzer informiert**
  - Mails werden nicht gelesen
  - RSS-Feed wird nicht gelesen
- **Ca. 1 Monat nach Scharfschaltung der Sperre:**
  Wenige „Meckerer“, diese aber umso intensiver
  → Vorgesetzte und Entscheider brauchen viel Rückgrat
- **Begründungen:**
  - Alte Formate werden zwingend benötigt
  - Zusammenarbeit mit externen Wissenschaftlern sonst nicht möglich
  - „Sicherheit“ sei nett, die Maßnahme aber völlig überzogen
  - „Mir ist noch nie etwas passiert“
  - Versuch, Sonderregelungen durchzusetzen
- **Informationen:**
  - RSS-Feed: https://www.uni-due.de/zim/rss/zim_sicherheit.rss
  - Startseite des ZIM: https://www.uni-due.de/zim/
- **Sehr aktive und produktive Spam-Melde-Kultur**
  Samples weiterleiten an hotline.zim@uni-due.de

E-Mail-Signatur und Zertifikate

- **Die allermeisten Probleme bei E-Mails lösen sich durch digitale Signaturen**
- **Zertifikat beantragen: https://pki.pca.dfn.de/uni-duisburg-essen-ca-g2/pub**
- **Anleitung: https://www.uni-due.de/zim/services/e-mail/konfigurationsanleitungen/zertifikat-anfordern**
- Kleines „aber“
  - Der Einrichtung von Zertifikaten ist etwas umständlich
  - Wiederherstellung des Zertifikats?
  - Umgang mit verschlüsselten Mails?
  - **Admins oder ZIM fragen!**

E-Mail-Signatur und Zertifikate

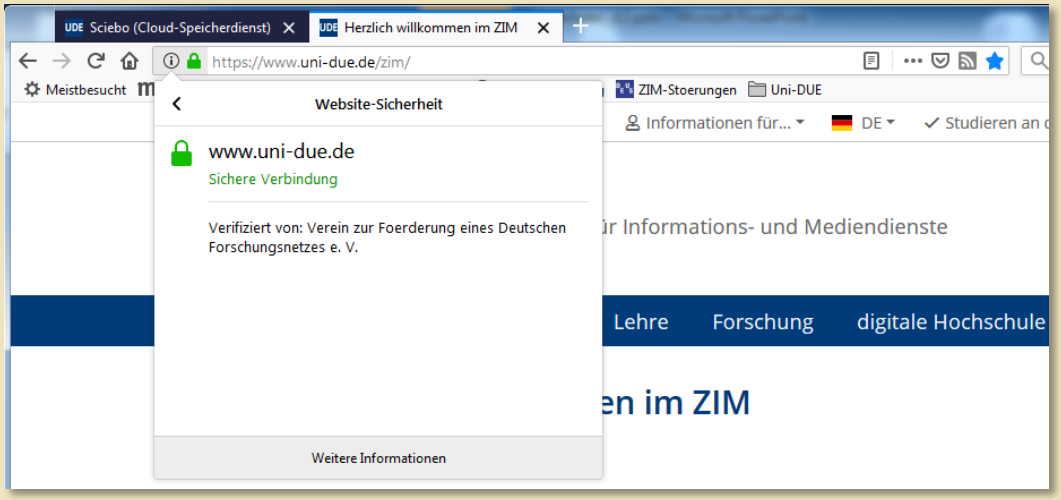
Nicht digital signiert:
Der Absender kann irgendwer sein, egal was dort steht



Digital signiert:
Der Absender ist der, als den ihn sein Zertifikat ausweist

E-Mail-Signatur und Zertifikate

- **Ca. die Hälfte der Phishing-Seiten nutzt https**
  - Zertifikate vom (gekaperten) Webhoster
  - LetsEncrypt
- **Wie unterscheiden sich Phishing-Seiten von legitimen Seiten?**
- **Bei der Gelegenheit: Serverzertifikate ebenfalls über DFN-Verein**
- **An DFN-Zertifikate kommen Angreifer nicht so leicht**
  → Gutes Unterscheidungsmerkmal



Browserabsicherung: Firefox

- **Nutze ich immer noch:**
  - uBlock Origin
  - Cookie AutoDelete
  - Privacy Badger
- **Neu dazugekommen:**
  - Smart Referer
  - I don‘t care about cookies

Sicherheit bei Auslandsreisen

- **Geräteverschlüsselung**
  - Immer sinnvoll
  - Laptops: Vollverschlüsselung per Bitlocker oder LUKS/LVM
  - Smartphones: SD-Karte nicht vergessen
- **Bei behördlichen Kontrollen nur begrenzt hilfreich**
- **Backup an anderer Stelle haben**
- **Ideal**
  - Leeres Gerät mitnehmen
  - Passwörter vorher ändern
  - Passwörter nach Rückkehr ändern
  - Gerät nicht aus den Augen lassen

Vorinstallierte Schadsoftware auf IT-Geräten

- **Warnung des BSI (Juni 2019)**

> Erneut hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf mehreren Smartphones vorinstallierte Schadsoftware nachgewiesen. Die Geräte wurden auf unterschiedlichen Online-Marktplätzen gekauft und auf eine bereits im Februar nachgewiesene Schadsoftware-Variante überprüft. Das BSI warnt daher auf Grundlage von ↗ §7 des BSI-Gesetzes vor dem Einsatz der Geräte Doogee BL7000 und M Horse Pure 1 und rät allen Anwenderinnen und Anwendern zu besonderer Vorsicht. Auch auf dem Gerät Keecoo P11 wurde die Schadsoftware in der Firmware-Version V3.02 (V362HH.SHWY.HB.HJ.P3.1130.V3.02) nachgewiesen. Für dieses Gerät steht eine Firmware V3.04 (V362HH.SHWY.HB.HJ.P3.0315.V3.04) ohne diese Schadsoftware über die Updatefunktion „Wireless Update" des Herstellers zur Verfügung. Daneben hat das BSI auf dem Gerät VKworld Mix Plus die gleiche Schadsoftware bei den Firmware-Versionen V3.05 (A5WNA23WKQ.RES.HB.HD.S8SCP8.0918.V3.05) und V3.07 (A5WNA23WKQ.RES.HB.HD.S8SCP8.1030.V3.07) nachweisen können, diese wurde allerdings nicht aktiv. Auch in diesen Fällen ist für Verbraucherinnen und Verbraucher besondere Vorsicht geboten.

Quelle: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/bsi-warnung-smartphones-060619.html

- **Besser auf (zu) günstige No-Name-Produkte verzichten**

Schnelles Backup unter Windows

- **Robocopy**
- **Sehr nützlich, sehr schnell**
- **Auf jedem Windows-System bereits vorhanden**

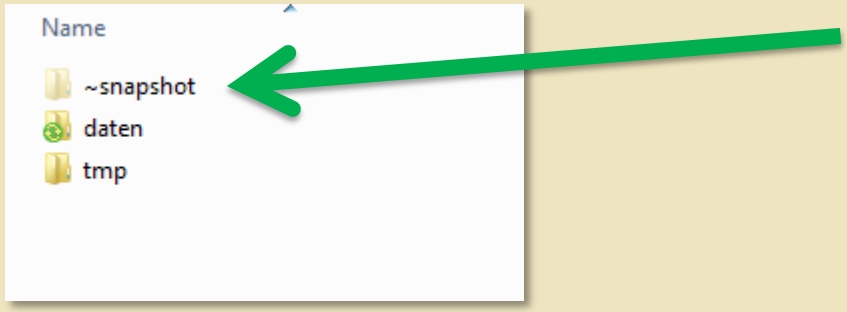
```
robocopy <Quelle> <Ziel> /E /Z /COPY:DAT /DCOPY:T /XJ
/X /V /NP /ETA /R:0 /W:5 /TEE /LOG+:<Logdatei>
```

- **Backups sind immer sinnvoll!**
- **Updates auch.**

Es gibt zwei Arten von Daten: Gesicherte Daten und unwichtige Daten

Vermischtes

- **Bildschirm sperren: Windows+L**
- **Netzlaufwerk: Automatische Snapshots nicht vergessen: ~snapshot**



- **Eigene Kennwörter niemals auf fremden Geräten eingeben**
- **Fremde USB-Sticks niemals an eigene Geräte anschließen**

Informationsquellen

- **Sicherheits-RSS-Feed**
  - https://www.uni-due.de/zim/rss/zim_sicherheit.rss oder
  - https://www.uni-due.de/zim
- **Meldungen und Fragen**
  - hotline.zim@uni-due.de
- **Digitale Zertifikate**
  - https://www.uni-due.de/zim/services/e-mail/konfigurationsanleitungen/zertifikat-anfordern
- **Datenaustausch**
  - Gigamove: https://www.uni-due.de/zim/services/gigamove.php
  - Sciebo: https://www.uni-due.de/zim/services/sciebo/
- **Test auf Datenlecks**
  - Have I been pwned? https://haveibeenpwned.com/
  - Hasso Plattner Institut: https://sec.hpi.de/ilc/

Informationsquellen

- **Sicherheits-RSS-Feed**
  - https://www.uni-due.de/zim/rss/zim_sicherheit.rss oder
  - https://www.uni-due.de/zim
- **Meldungen und Fragen**

Vielen Dank für Ihre Aufmerksamkeit!

- **Datenaustausch**
  - Gigamove: https://www.uni-due.de/zim/services/gigamove.php
  - Sciebo: https://www.uni-due.de/zim/services/sciebo/
- **Test auf Datenlecks**
  - Have I been pwned? https://haveibeenpwned.com/
  - Hasso Plattner Institut: https://sec.hpi.de/ilc/