IT-Sicherheit

Schulung für alle

Sensibilisierung, Erkennung, Abwehr von Cyber-Kriminalität

… wie Sie sich selbst schützen und gleichzeitig die Hochschule

Vorstellung

ETuQuali

Projekt bis Ende Juli 2024, gefördert von der Stiftung Innovation in der Hochschullehre, bildet an der Pädagogischen Hochschule E-Tutor*innen aus

MIT

Zentrum für
Medien und Informationstechnologie
der Pädagogischen Hochschule Ludwigsburg

gefördert von der
Stiftung
Innovation in der
Hochschullehre


WAS ZUR...?!
EIN VIRUS SAGEN SIE?
DA KOMM ICH GLEICH VORBEI...
IT Support
HAHA! GROSSARTIG, UND SIE SIND SICHER, DASS ICH DAS ENTFERNEN SOLL?!
IT Support
ZING
ZING
ITCOMICS.DE

Warum bin ich eigentlich hier?

kontinuierlicher Anstieg
Cyberkriminalität in den letzten Jahren

zusätzliche Bedrohung
durch Homeoffice/ Mobile Workplaces/ “Cyberwar”

zunehmende Professionalisierung
der Angreifer

social engineering
vermehrt Ausnutzung menschlichen Verhaltens

öffentliche Einrichtungen und Hochschulen
im Fokus und vermehrt Ziele von Angriffen

In den vergangenen Jahren haben massive Angriffe auf Hochschulen mit teilweise langanhaltenden Folgen stattgefunden

Ansbach | Berlin | Chemnitz | Dresden | Essen | Freiburg | Gießen | Heilbronn | Ilmenau | Jülich | Köln | Leipzig | Münster | Nürnberg | Osnabrück | Pforzheim | Q* | Ruhr-West | Stuttgart | Tübingen | Ulm | Villingen-Schwenningen | Weingarten | X* | Y* | Zwickau

*in diesen Städten gibt es keine Hochschulen

Wer macht denn sowas?

oder:

Warum Ihre Mithilfe wirklich wichtig ist, damit die Hochschule (und Sie) nicht gehackt werden

keine Einzelpersonen (Nerds)
Die guten alten Zeiten sind vorbei!

Globalisierung - international, zum Teil staatlich unterstützt
Hackergruppen

Professionalisierung
extreme Professionalisierung + Hilfestellung bei der "Lösegeldübergabe"

Spezialisierung
und Arbeitsteilung

Lange vorbereitet und hochkomplex
z.B. SunBurst, 2 Jahre Vorbereitung, Beteilung von über 1000 Personen (laut Microsoft)

Wieso hackt man denn eine Hochschule?

oder:

Warum Ihre Mithilfe wirklich *richtig* wichtig ist, damit die Hochschule (und Sie) nicht gehackt werden

Ziele

Erpressung von Lösegeld
Verschlüsselte Daten, Veröffentlichung von gestohlenen Daten

Daten, Technologiediebstahl
Ausspähen von Betriebsgeheimnissen (Pharma, Autoindustrie, Forschungsergebnisse ...)

Rechenleistung (Crypto-Mining)
CO2 von Crypto-Mining in China > kompletter Energiebedarf von Tschechien

Identitätsdiebstahl
Übernahme von Accounts (Mail, Amazon, Instagram, Facebook, Spam ...)

Vortäuschung von Geschäftsvorgängen
z.B. Bezahlen einer Rechnung ins Ausland

Ziele

zunehmend Verlagerung auf
"Big Players", öffentliche Einrichtungen und kritische Infrastruktur

Vandalismus
reine Zerstörungswut

Beliebigkeit
“zur falschen Zeit am falschen Ort” oder absolute Willkür

trotzdem ist man auch als kleines Unternehmen, Verein oder Privatperson nicht sicher!

Und was machen die dann damit?

oder:
Warum Ihre Mithilfe wirklich *so* richtig wichtig ist, damit die Hochschule (und Sie) nicht gehackt werden

z.B. Verkauf im “Darknet”

Kreditkartendaten mit Belastungslimit bis 5000 €
im Darknet für umgerechnet 20 $

Online-Banking-Daten
im Darknet für umgerechnet 35 $

Europäischer Reisepass
im Darknet für umgerechnet 1500 $

Hacken eines Instagram-Accounts
im Darknet für umgerechnet 56 $

Einstündige DDoS-Attacke ("Serverüberlastung")
im Darknet für umgerechnet 10 $

Das ist doch der Job der IT-Abteilung!?

oder:

Warum Sie echt wichtig sind und die Hochschule schützen können

Zugriffspunkte für Hacker z.B. in ein Hochschulnetzwerk

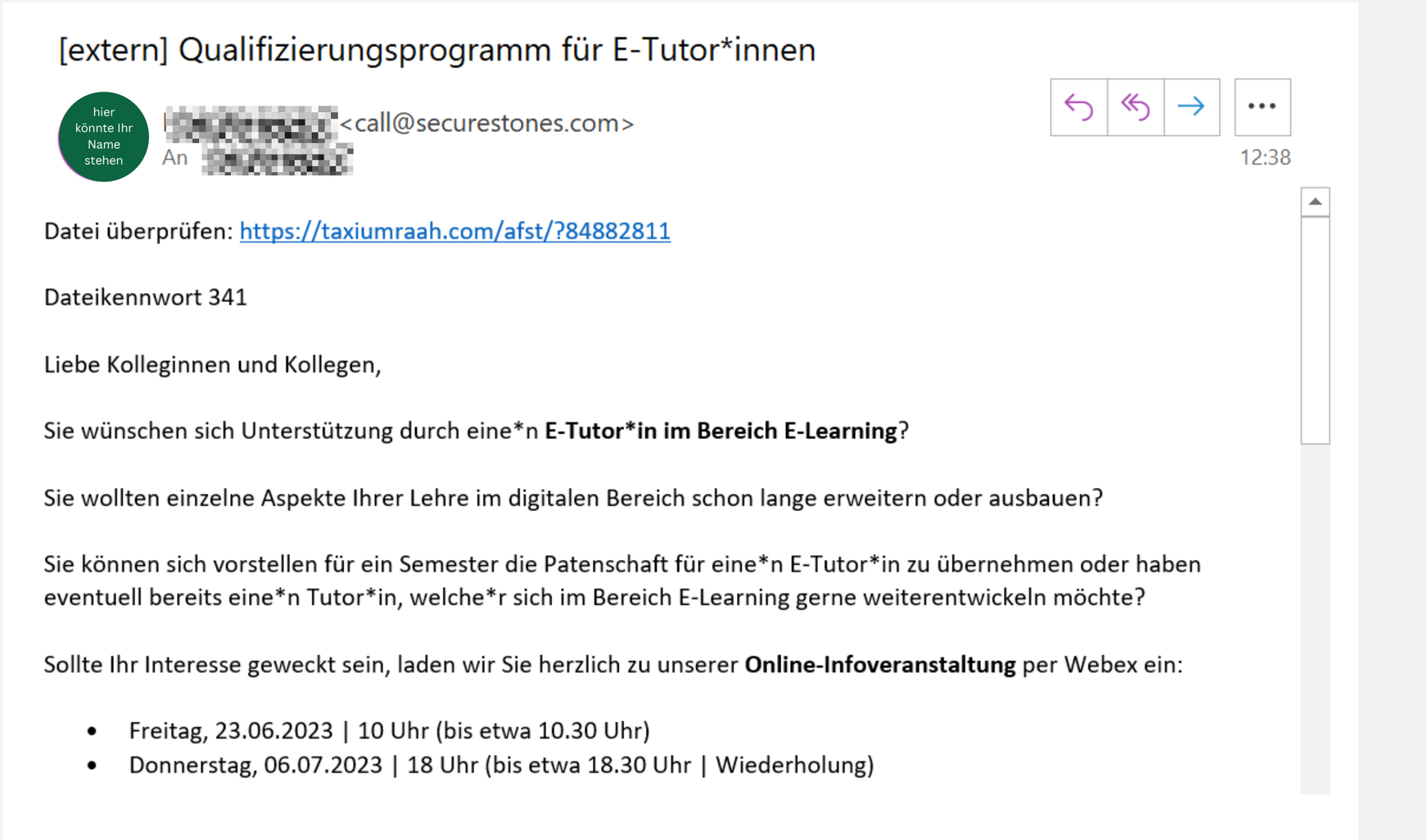
- Sicherheitslücken in öffentlich zugänglichen Diensten (OWA; RDP usw.)
- Fernzugriff (VPN, Citrix, RDP) mit gestohlenen/ erratenen Kennwörtern
- unsicheres WLAN
- physikalischer Zugang zu Netzwerkgeräten (Windows + L)
- USB-Sticks/CDs
- Social Engineering (E-Mail, Telefon)
- kompromittierter Mitarbeiter

Wie wird eine Hochschule gehackt?

oder:

Warum Sie automatisch die Hochschule schützen, wenn Sie sich schützen - und andersrum

Kurzer Einblick in die Praxis



[extern] Qualifizierungsprogramm für E-Tutor*innen

hier könnte Ihr Name stehen

[redacted] <call@securestones.com>

An [redacted]

12:38

Datei überprüfen: https://taxiumraah.com/afst/?84882811

Dateikennwort 341

Liebe Kolleginnen und Kollegen,

Sie wünschen sich Unterstützung durch eine*n **E-Tutor*in im Bereich E-Learning**?

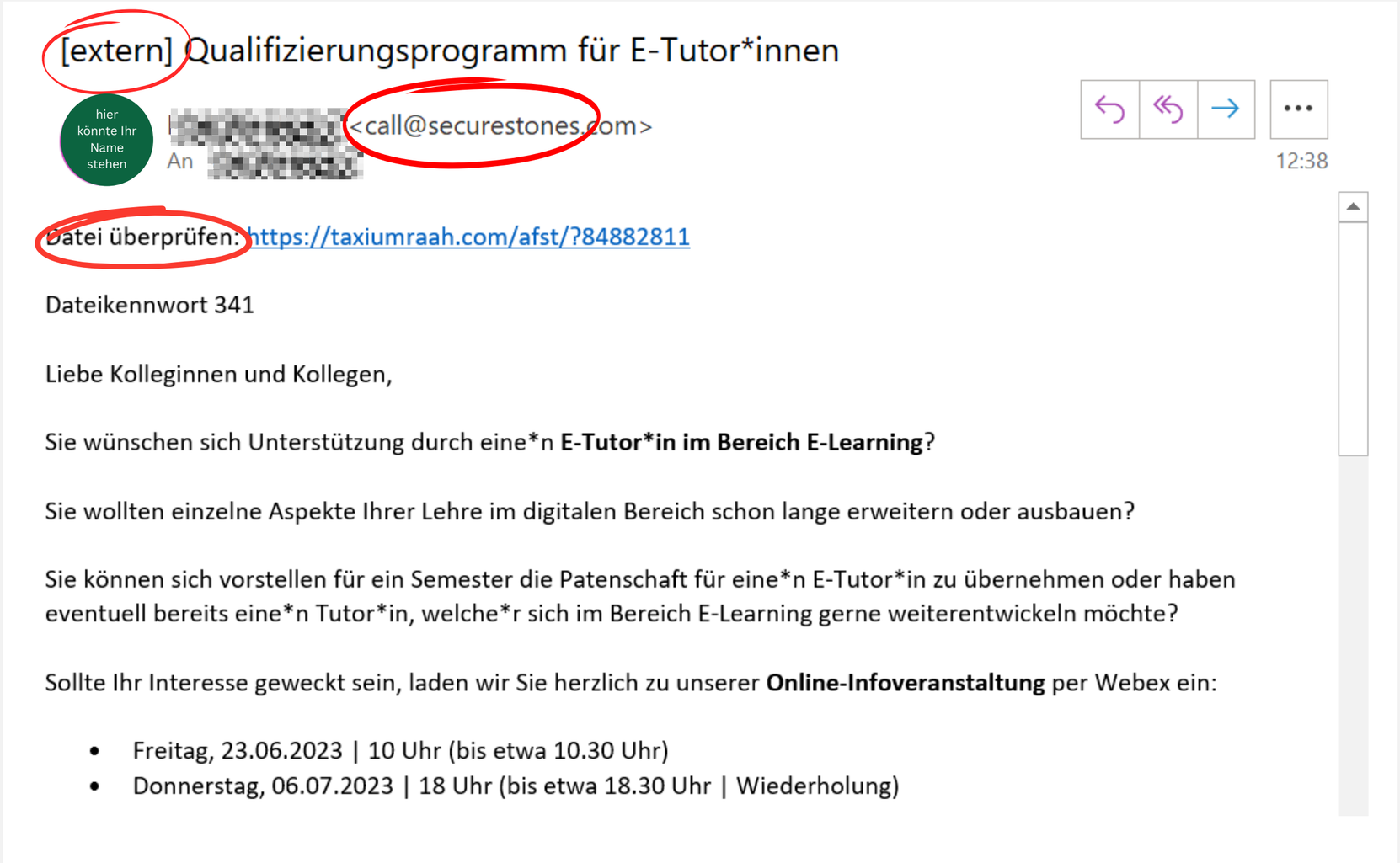
Sie wollten einzelne Aspekte Ihrer Lehre im digitalen Bereich schon lange erweitern oder ausbauen?

Sie können sich vorstellen für ein Semester die Patenschaft für eine*n E-Tutor*in zu übernehmen oder haben eventuell bereits eine*n Tutor*in, welche*r sich im Bereich E-Learning gerne weiterentwickeln möchte?

Sollte Ihr Interesse geweckt sein, laden wir Sie herzlich zu unserer **Online-Infoveranstaltung** per Webex ein:

- Freitag, 23.06.2023 | 10 Uhr (bis etwa 10.30 Uhr)
- Donnerstag, 06.07.2023 | 18 Uhr (bis etwa 18.30 Uhr | Wiederholung)

Aber die ist doch echt?!



[extern] Qualifizierungsprogramm für E-Tutor*innen

hier könnte Ihr Name stehen

[redacted] <call@securestones.com>

An [redacted]

12:38

Datei überprüfen: https://taxiumraah.com/afst/?84882811

Dateikennwort 341

Liebe Kolleginnen und Kollegen,

Sie wünschen sich Unterstützung durch eine*n **E-Tutor*in im Bereich E-Learning**?

Sie wollten einzelne Aspekte Ihrer Lehre im digitalen Bereich schon lange erweitern oder ausbauen?

Sie können sich vorstellen für ein Semester die Patenschaft für eine*n E-Tutor*in zu übernehmen oder haben eventuell bereits eine*n Tutor*in, welche*r sich im Bereich E-Learning gerne weiterentwickeln möchte?

Sollte Ihr Interesse geweckt sein, laden wir Sie herzlich zu unserer **Online-Infoveranstaltung** per Webex ein:

- Freitag, 23.06.2023 | 10 Uhr (bis etwa 10.30 Uhr)
- Donnerstag, 06.07.2023 | 18 Uhr (bis etwa 18.30 Uhr | Wiederholung)

PHising

oder:

Kann das echt so stimmen?

1. klassisch

große Massen an E-Mails
"Herzlichen Glückwunsch, Sie haben gewonnen"

wenig Individualität
"Lieber Kunde, erhalten Sie sofort Rabatt, wenn Sie hier klicken!"

oft leicht zu erkennen
"Hallo Müller, ich beobachte dich"

Ansprache, Stil, Form, Rechtschreibung verdächtig
"Die DLH liefert ihr Paket heute nur, wenn sie ihr klicken"

Von: leafein <afakstudy@gmail.com>
Gesendet: Donnerstag, 10. August 2023 10:32
An: [redacted] Dekanat Fakultät 3
Betreff: [extern] Hi. wollte mich mal wieder bei dir melden.

Das ist schon toll!
http://0mT.seemsurvive.co.in/34546de4235m342356?affsub2=8xHx6yyk5&st=8/10/2023 1:32:36 AM

In Erwartung deiner Nachricht,leafein

2. spear

gezielter Angriff auf einen einzelnen
"Sehr geehrter Herr XY, im Rahmen Ihres Projektes soundso..."

Analyse alter Mails
Gehen Sie davon aus, dass Angreifer Zugriff auf die Mails von Studierenden haben

Informationen über Opfer
social media, Unternehmens-Websiten, Netzwerke wie LinkedIn

Thematisieren von echten Vorgängen und Imitation von Form und Stil
“Liebe XY, für unseren Drittmittelantrag fehlt uns noch ein Finanzierungsplan.
Hier mein Vorschlag im Anhang.”

Пн 09.12.2019 18:57

Verdächtiger Absender

AmazonWebService <no-reply@amazon-sec.com>

Suspicious Activity Detected!

To [redacted]

amazon

Dear [redacted]

Case ID : **2887655768,**

Four your safety, your Amazon has been locked because we found some suspicious activity on your account. Someone accessing your account and make some change on your account information. This the details :

Country	:	Dominica
IP Address	:	64.250.251.208
Date and Time	:	09/12/2019 15:59:36
Browser	:	Google Chrome

If you did not make these action or you believe an unauthorized person has accessed your account, you should login to your account as soon as possible to verify your information.

3. whale

gezielter Angriff auf einen "big fish"
Hochschulleitung, Buchhaltung, Geschäftsführung

CEO Fraud
Angreifer gibt sich als Hochschulleitung aus und fordert Finanzabteilung an, Geld zu überweisen o.ä.

4. voice

Telefonanruf
"Guten Tag, hier der Support von Microsoft, ..."

Vertrauensbildend durch persönliche Ansprache
"Guten Tag Frau XY, hier der neue Azubi vom MIT"

Druckausübung
"ich sehe, dass Sie einen Virus auf Ihrem Rechner haben, den wir ganz schnell entfernen müssen, da sonst alle Ihre Daten gelöscht werden!"

Künstliche Intelligenz: Deep Fake
Stimmengenerator, der mithilfe z.B. öffentlich zugänglicher Sprachbeispiele jeden alles sagen lassen kann - der neue “Enkeltrick”

5. SMS

SMS mit Links
Smartphones: "Link zur Paketverfolgung..."

speziell codierte SMS
dadurch Fernsteuerung des Telefons

Fälschung der Absender-Nummer
Umleitung über andere Nummer (siehe Campustelefone)

auch bei SMS gilt dasselbe wie bei Mails, zudem:
WhatsApp o.ä., facebook-messenger, zoom, ...

Und wie genau geht das nun?

oder:
die Technik, die man als Hacker kennen sollte

1. Anhang der Mail

infizierte Datei im Anhang
"Im Anhang finden Sie die Rechnung für Ihre Bestellung des Whirlpools..."

ZIP-Datei
evtl. versteckt

enthält Makros oder andere ausführbare Skripte
diese laden dann die eigentliche Schadsoftware von einem C&C-Server nach

2. Fake-Login-Seite

- täuschend echt nachgebaut
- Eingabe von Benutzername und Kennwort
- Benutzerkonto wird vom Angreifer übernommen
- oftmals viele Wochen/ Monate unentdeckt
- Übernahme weiterer Systeme (gleiche Kennwörter)
- Nutzung des Kontos für Angriffe auf Bekannte/ Geschäftspartner
- "Identitätsdiebstahl"

Darauf fall ich doch nicht rein!

oder:
wie eine IT-Sicherheitsfirma 2023 gehackt wurde

Ködermethoden

- Mitteilung “unter Kollegen” (Abstimmung über Geburtstagsgeschenk, Spendensammlung ...)
- Offizielle Mails (E-Tutor*innen, Sicherheitsupdates, ...)
- CEO Fraud (seltsam nur, dass der Chef mich auf einmal duzt und keine Tippfehler macht...)
- Bezugnahme auf aktuelle Vorgänge (Bestellungen, Rechnungen,...)
- Nutzung allgemein bekannter Brands (DHL, PayPal, Telekom, Microsoft, Banken...)
- persönliche Notlagen (Tochter ruft an - Handy geklaut, ...)
- Drohszenarien (Ihr Postfach ist voll!)

Wie fall ich darauf nicht rein?

oder:
wie Sie sich (und die Hochschule) schützen

Prüfen

Stimmt die Rechtschreibung, Ausdruck, passt der Stil?
"Yo, Rektor. Schick mal das felende Geld zu uns!"

Inhalt und Plausibilität
Ich habe doch gar nichts bestellt?!?

Mailadressen
@phlubwigsbugr.de | telekom@info.ph

Links
www.nutzerkontoaendern-phludwigsburg.com

URL und Zertifikat von Login-Eingabemasken
sieht das richtig aus?

Ruhe bewahren

der angezeigte Link kann sich vom Echten unterscheiden
Link-Generator (Test: mit der Maus ohne zu klicken über den Link fahren)

die angezeigte Mailadresse kann sich von der Echten unterscheiden
max.mustermann@phlb.fi

Auch Anhänge können gefälscht/ verfälscht worden sein
Schickt mir diese Person wirklich einen Anhang?

gesundes Misstrauen bewahren, v.a. wenn...
Druck aufgebaut wird, es dringend/ geheim ist, es um Geld/ PW/ PINs und Kreditkarten geht

Absichern oder Rückfragen stellen
bei Ihnen bekannten Personen ("Codewort für Familie?")

Seriosität

Seriöse Partner fragen nicht nach Kennwörtern, PINs usw.
Ausnahme: die offizielle Login-Seite des Anbieters
TIPP: offizielle (sichere) Seiten als Favorit im Browser speichern

Lassen Sie keine unbekannten Personen an oder auf Ihren PC
auch nicht, wenn er sich als Techniker des MIT vorstellt...

Vorsicht bei USB-Sticks, CDs usw.
schon das Einlegen/Einstecken kann zur Infektion führen ("AutoRun")

Links/ URL/ Zertifikat prüfen

Wo führt mich der Link hin?
mit der Maus über den Link fahren OHNE zu klicken - die letzten beiden Teile des Links sind maßgeblich

Nur HTTPS ist verschlüsselt
vorne in der Adresszeile im Browser zu finden

Vorsicht!
HTTPS ist aber trotz Verschlüsselung nicht automatisch vertrauenswürdig

Tricks und Tipps

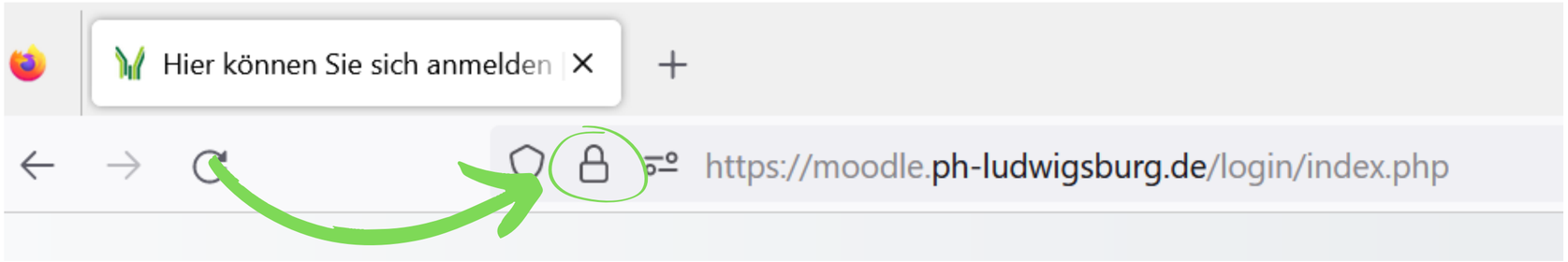
oder:
Handlungsempfehlung

So erkennen Sie “gefährliche” Links

- Fahren Sie mit der Maus über den Link, ohne zu klicken.
- Die letzten Teile des Links sind entscheidend.

So prüfen Sie ein Zertifikat

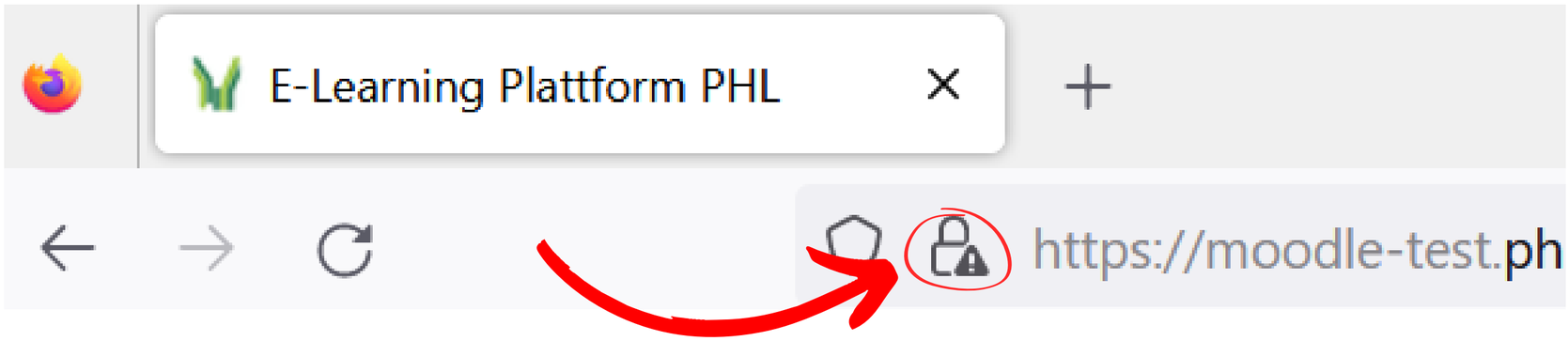
- Beachten Sie das Schloss in der Adresszeile des Browsers
- Klicken Sie darauf.
- Klicken Sie hier nun auf “Verbindung”.
- Sie werden nun darüber informiert, ob die Verbindung sicher ist.



Beispiel aus Firefox

Zertifikat nicht sicher

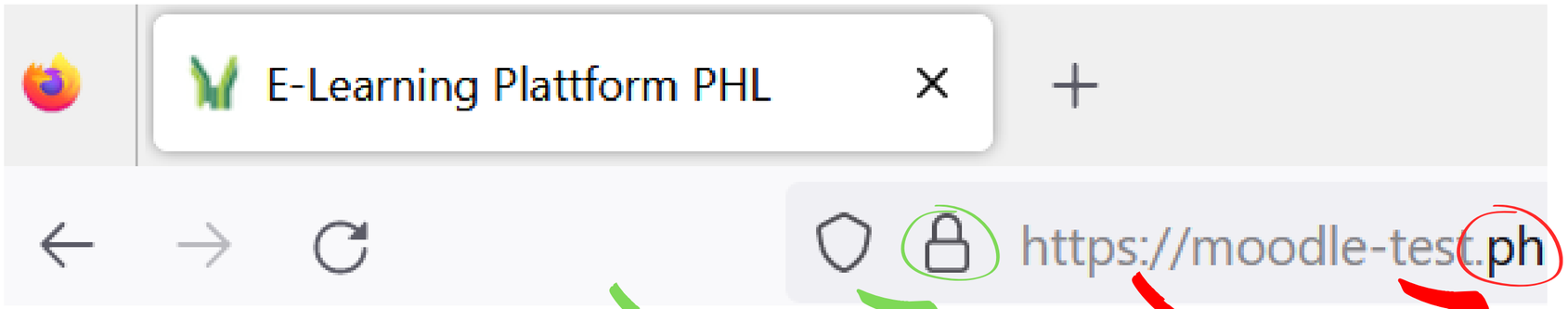
- Beachten Sie das Schloss in der Adresszeile des Browsers
- Hier sehen Sie nun ein Warndreieck neben dem Schloss (oft auch rot gefärbt)



Beispiel aus Firefox

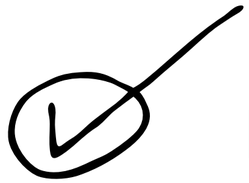
Zertifikat gefälscht

- Der Angreifer hat sich zu seiner Fake-Seite ein Fake-Zertifikat erstellt.
- Es wird kein Sicherheitsproblem erkannt.
- Sie erkennen jedoch, dass die Endung des Links seltsam ist

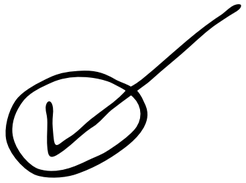


Beispiel aus Firefox

Seite ist (vermutlich) sicher



Die im Browser angezeigte URL stimmt.



Das Zertifkat-Symbol (Schloss) ist ok.

Tipp

Speichern Sie sich Seiten als Favorit
und nutzen Sie diese immer!

Tippen Sie Links selbst ein statt einfach vertrauensvoll auf Links zu klicken.

So schützen Sie sich vor falschen Mails

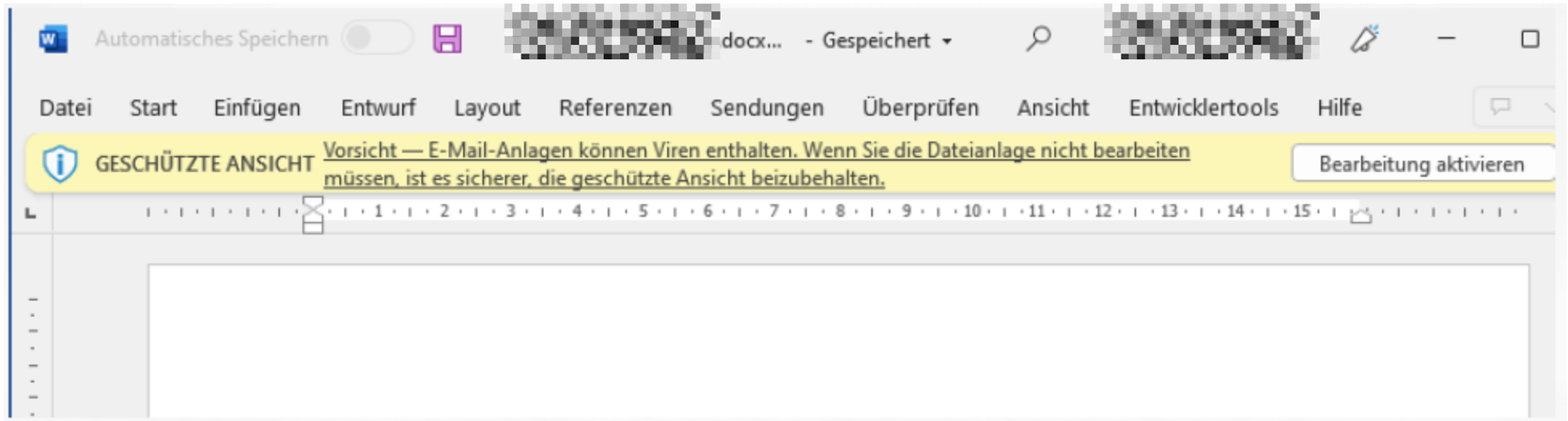
- Prüfen Sie immer, welche Mailadresse angegeben ist.
- Fahren Sie mit der Maus über die Mailadresse ohne zu klicken.
- Die letzten beiden Teile der Mailadresse sind entscheidend (z.B. @fake.ru)
- Die echte Mailadresse ist i.d.Regel in spitzen Klammern angegeben.

So schützen Sie sich vor Dateianhängen

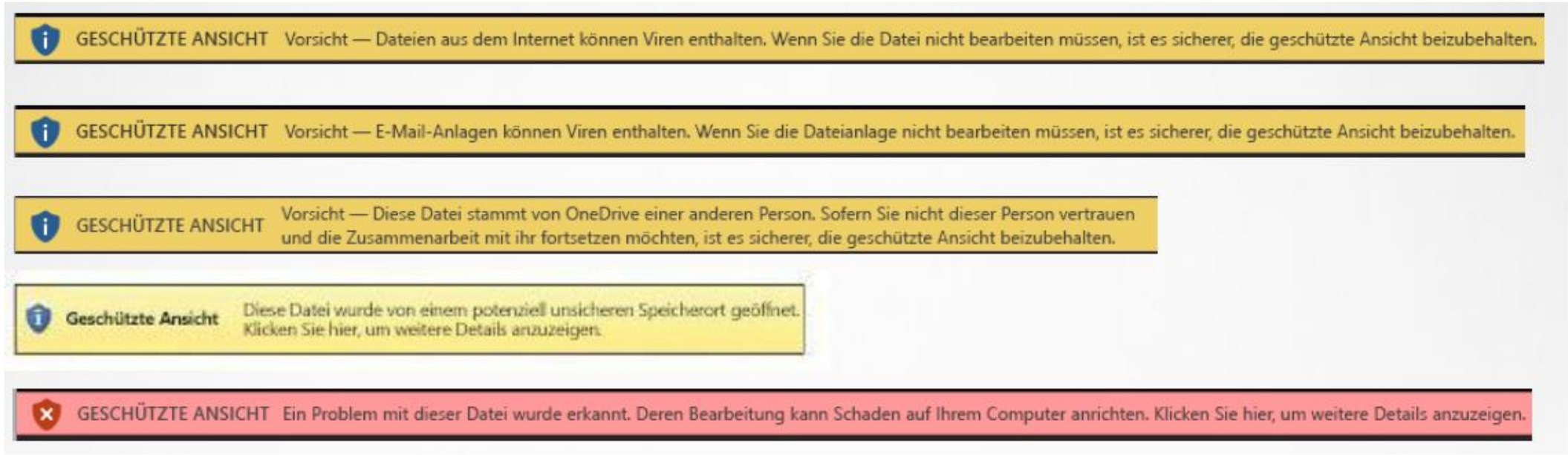
- Direkt ausführbare Dateien sind immer gefährlich (.com, .exe, .cmd, .msc, .sfc,...)
- Makros sind gefährlich (vereinfachen Arbeitsschritte, z.B. in Excel, durch Automatisierung - ppt/doc/docm/...)
- Read-only normalerweise in Ordnung
- Vorsicht bei Archivdateien und pdfs! Hier kann sich z.B. ein Virus im “Container” verstecken.
- Prüfen Sie auch Links innerhalb PDFs.

Behalten Sie die geschützte Ansicht bei Office bei

- Beachten Sie die dortigen Sicherheitsmeldungen (oben im gelben Hinweisfeld)
- Klicken Sie nicht unvorsichtig auf “Bearbeiten aktivieren”.

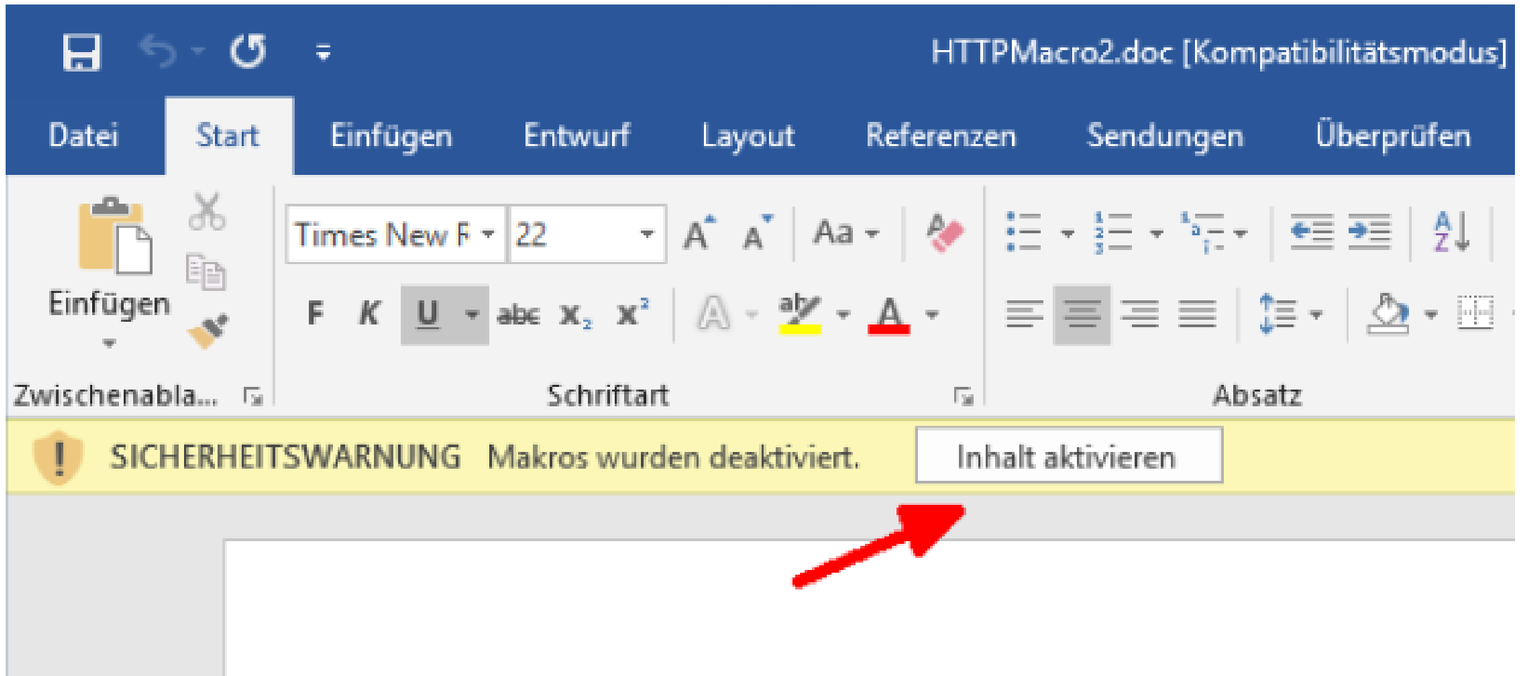


Behalten Sie die geschützte Ansicht bei Office bei



Beachten Sie Sicherheitsmeldungen für Makros

- Deaktivieren Sie diese Funktion nicht.
- Beachten Sie die Sicherheitsmeldungen.
- Klicken Sie nicht unvorsichtig auf “Bearbeiten aktivieren”.



Agieren Sie selbst verantwortungsbewusst!

- Geben Sie Passwörter nur an Menschen weiter, denen Sie auch Ihre Kreditkarte und Ihre Bank-Pin weitergeben würden.
- Verwenden Sie selbst bei Links nur Klarlinks (kein “bitte hier klicken” als Link).
- Prüfen Sie, ob der Virenscanner auf Ihrem Dienstrechner aktuell und funktionsfähig ist (neuer Virenscanner: BitDefender)

Zusammengefasst

- Bleiben Sie argwöhnisch und achtsam.
- Öffnen Sie keine unbekannten Anhänge und Mails.
- Fragen Sie lieber noch einmal persönlich bei Kolleg*innen nach.
- Leiten Sie seltsame Mails lieber einmal mehr an **virusverdacht@ph-ludwigsburg.de** weiter.
- Vereinbaren Sie ein Codewort für Telefonanrufe mit nahen Bekannten/Familie.
- Verwenden Sie selbst keine “unseriösen Techniken” (PW weitergeben,...).

Was mache ich,
wenn’s doch mal passiert?

Das kann jedem passieren

z.B. versehentlich Datei geöffnet und leeres Word-Dokument öffnet sich

- Ruhe bewahren - das passiert den Besten.
- Schalten Sie den Laptop sofort aus (z.B. Aus-Schalter mehrere Sekunden gedrückt halten)
- Informieren Sie die IT-Abteilung (**mit@ph-ludwigsburg.de** oder Telefon +49 (0) 7141 140 **2999**).
- Versuchen Sie nicht, den Vorfall “auszusitzen” - je schneller Sie reagieren, umso schneller kann ein evtl. Schaden begrenzt werden!

Wie schütze ich durch meine Vorsicht nun die Hochschule?

oder:
die Bedeutung eines jeden einzelnen

- Auch Privatpersonen werden angegriffen (derzeit z.B. Routernutzung durch Hacker zur Identitätsverschlüsselung).
- Lösegeldforderungen i.d.Regel geringer
- Vom Homeoffice an die Hochschule - Einschleppen von Viren, Öffnen von Zugriffspunkten

Best Practice

oder:
wie ich mich zusätzlich schützen kann

Schützen Sie sich und uns!

- Trennen Sie Berufliches und Privates (v.a. bei Mailadressen etc.)!
- Geben Sie auf Social Media so wenig wie möglich preis, nutzen Sie entsprechende strenge Privatsphäre-Einstellungen
- Updaten Sie Ihren Rechner regelmäßig (Systemupdate). Warten Sie nicht mit Updates.
- Sorgen Sie für einen guten Virenschutz/ Virenscanner.
- Nutzen Sie unterschiedliche Accounts (NormalerUser + Admin für Installationen)
- Erstellen Sie für jeden Nutzer des PCs einen eigenen Nutzeraccount.
- Sorgen Sie für ein regelmäßiges BackUp, welches auch offline verfügbar ist (“air-gap”).
- Verwenden Sie sichere Passwörter (nicht “hallo123”) und notieren Sie diese nur mithilfe z.B. des Keepasses.

Schützen Sie sich und uns!

9. Lesen Sie Mails im Textformat (in Outlook: Datei - Optionen - TrustCenter | “Einstellungen für das TrustCenter” bestätigen | E-Mail-Sicherheit - als Nur-Text lesen: Option “Standardnachrichten im Nur-Text-Format lesen” ankreuzen).
10. Verwenden Sie verschlüsselbare USB-Sticks (kostenfrei erhältlich beim MIT - datashur) bzw. eine Bitlocker-Verschlüsselung.
11. Melden Sie Phisingmails an **virusverdacht@ph-ludwigsburg.de** (einfach kommentarlos weiterleiten).
12. Misstrauen Sie jeder Mail - wichtigen erst recht!
13. Verwenden Sie verschiedene Kennwörter.
14. Schalten Sie Sicherheitswarnungen nicht ab.
15. Vermeiden Sie öffentliche (v.a. ungesicherte offene) Netzwerke.

Diese und weitere ausführliche Informationen sowie Anleitungen
(inkl. aller aktuellen Warnhinweise) finden Sie auch unter:
https://www.ph-ludwigsburg.de/hochschule/einrichtungen/mit/it-sicherheit