Folgende Regeln helfen Ihnen, betrügerische Nachrichten zu erkennen

1. **Regel:** Prüfen Sie jede empfangene Nachricht auf korrekten Absender und Inhalt:
   - Passt der Absender nicht zur Nachricht?
     - ✓ Der Absender awareness@hwr-berlin.de ist bei einer HWR-internen E-Mail plausibel.
     - ✗ Der Absender awareness@xyz.de ist bei einer HWR-internen E-Mail **nicht** plausibel.
   - Werden sensible Daten abgefragt?
   - Erhalten Sie eine Zahlungsaufforderung die keinen Sinn ergibt?
   - Erwartet jemand von Ihnen einen Rückruf, zu einer in der Mail angegebenen Rufnummer?
   - Erhalten Sie Mails von einer Seite auf der Sie kein Nutzerkonto haben?
   - Erhalten Sie die Nachricht unerwartet?
   - Ist die Anrede eher neutral gehalten?
   - Ist die E-Mail von der entsprechenden Person nicht digital signiert?

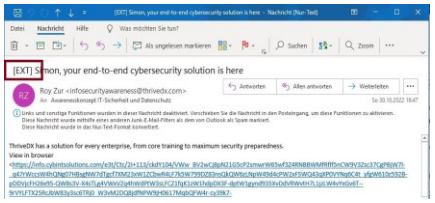
Sollten Sie einige dieser Fragen mit „Ja“ beantworten, dann handelt es sich vermutlich um eine schadhafte Mail. Gerade wenn von Ihnen Kontoinformationen oder Passwörter verlangt werden, sollten Sie misstrauisch werden.

Mitarbeiter der HWR Berlin einschließlich der IT fragen Sie niemals nach Ihrem Passwort.

Übrigens: Nach dem gleichen Prüfschema können Sie auch bei anderen Kommunikationsmitteln, insbesondere Telefonanrufen, vorgehen.

2. **Regel:** Prüfen Sie jede Nachricht, ob ein [EXT] enthalten ist.

Alle Absender, die vorgeben eine Abteilung oder Funktion von innerhalb der HWR Berlin zu sein und ein [EXT] in der Betreffzeile der Email aufweisen, wurden von außerhalb der HWR Berlin verschickt. Das bedeutet, dass jemand vorgibt von der HWR



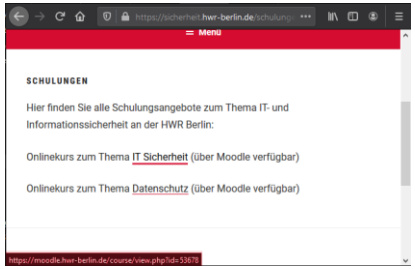
Berlin zu sein. Es handelt sich in diesem Fall nahezu immer um eine Phishing-Mail.

3. **Regel:** Die erhaltene Mail besteht die erste Überprüfung und scheint eine legitime Mail zu sein?

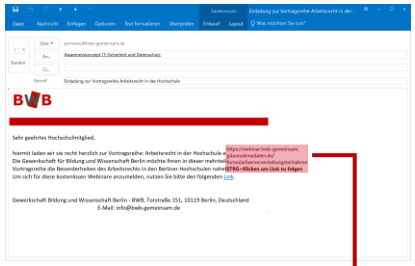
Dann geht es nun daran, mögliche Links in der E-Mail auf deren wahre Zieladresse zu prüfen. Eventuell wurde Ihr Kommunikationspartner gehackt und die Mail kommt tatsächlich vom Mail-Account des (internen) Absenders. In diesem Fall wirken Absender und möglicherweise auch Inhalten zunächst legitim.

Die meisten Links erkennt man daran, dass Sie in blauer Schrift geschrieben und unterstrichen sind. Gut manipulierte Mails passen den Link allerdings an die restliche Mailformatierung an, daher müssen Sie dort aufmerksam sein.

Um einen Link auf seine wahre Zieladresse zu prüfen, müssen Sie wissen an welcher Stelle Ihnen die Adresse hinter dem Link angezeigt wird. Je nach Programm oder Service befindet sich die Anzeige an unterschiedlichen Stellen.



Hier sehen Sie die Zieladresse in der Statusleiste des Webbrowsers.



Hier sehen Sie die Zieladresse im Tooltip von Outlook.

Wenn Sie mit der Maus über einen Link fahren, wird in der Regel in der Statusleiste von Outlook oder Ihrem Browsers die Zieladresse des Links eingeblendet. Bei Outlook öffnet sich zusätzlich ein kleines Hinweisbanner - auch Tooltip genannt.

Bei mobilen Geräten wie Smartphones oder Tablets, gibt es ebenfalls die Möglichkeit einen Link zu prüfen. Wir empfehlen Ihnen jedoch eine Überprüfung von Links nur an einem Desktoprechner oder Laptop durchzuführen, da mobile Geräte lediglich über sehr kleine Displays verfügen.

Regel: Sobald Sie die Zieladresse eines Links kennen, gilt es die Domain zu analysieren und damit zu bestimmen, ob ein Klick auf den Link sicher ist.

https://www.it.hwr-berlin.de/helpdesk/
Domain

Die Domain einer Webadresse (in diesem Fall hwr-berlin.de) befindet sich immer vor dem ersten Schrägstrich „/“. Sie besteht üblicherweise aus einem Wort und einer Top-Level-Domain, die durch einen Punkt „.“ getrennt werden. Die Top-Level-Domain kennen Sie als Endung (z.B. .de, .com, .org, .net, etc.). Die Domain ist das wichtigste Mittel um zu bestimmen ob eine Nachricht einen schadhaften Link enthält. Es kann vorkommen, dass statt einem Namen in der Domain nur Ziffern stehen, die sogenannte IP-Adresse. Alle Webseiten haben eine IP-Adresse, um die Benutzung im Alltag zu vereinfachen, wurden die Domains eingeführt. Sollten Sie einen Link mit einer IP-Adresse erhalten, dann handelt es sich mit hoher Wahrscheinlichkeit um einen schadhaften Link.

✗ https://192.168.2.1/hwr-berlin.de

Übrigens: Das „S“ in https steht für „Sicher“, dabei handelt es sich allerdings nur um die Verbindung zur Webseite und nicht um den Inhalt. Kriminelle nutzen https daher gerne um Ihnen Sicherheit vorzugaukeln.

Regel: Haben Sie die Domain identifiziert, müssen Sie prüfen ob diese Domain zum Absender oder dem Inhalt der Mail passt. Die richtige Schreibweise der Domain ist dabei auch entscheidend. Erhalten Sie z.B. eine Mail „Ihrer“ Bank, muss die Domain auch die Domain sein, die zu Ihrer Bank gehört. Ist die Domain im Link hier abweichend, klicken Sie keinesfalls auf den Link.

Im Fall, dass Sie z. B. erwarten, dass der Link Sie zur HWR Berlin führt:

✓ https://it.hwr-berlin.de/helpdesk
✗ http://it.hwr.de/login

Übrigens: Bei Betrügern ist es beliebt, die richtige Domain an eine andere Stelle im Link zu schreiben um Sie zu täuschen:

✓ https://www.hwr-berlin.de/
✗ https://www.hwr-berlin.de.hwrberlin.de/
✗ https://hwrberlin.de/hwr-berlin.de
✗ https://hwr-berlin.de.hwr.de/helpdesk

Übrigens: Beliebt bei Angreifern ist es, Abwandlungen der Domain zu registrieren. Dabei hoffen Betrüger, dass Sie nicht aufmerksam genug lesen und eine Vertauschung von zwei Buchstaben nicht bemerken:

✓ https://www.hwr-berlin.de/
✗ https://www.hrw-berlin.de/
✗ https://www.hwr-beriin.de/
✗ https://www.hwr-ber1in.de/

Regel: Haben Sie die Domain ermittelt, können aber nicht sagen ob die Domain legitim ist, dann klicken Sie bitte nicht auf den Link, sondern nutzen eine Suchmaschine um sich über diese Adresse zu informieren.

✓ https://www.hwr-berlin.de/
✗ https://www.hwr-studium.de/

Regel: Sollte eine Nachricht alle vorherigen Prüfungen bestanden haben, ist es weiterhin möglich, dass es sich hierbei um eine schadhafte E-Mail handelt. Die E-Mail könnte von einem gehackten Account kommen, daher ist es wichtig die möglichen Dateianhänge zu prüfen, bevor diese angeklickt werden:

- Direkt ausführbare Dateiformate (sehr gefährlich): z. B. .exe, .bat, .com, .cmd, .scr, .pif
- Dateiformate, die Makros enthalten können: z. B. Microsoft Office Dateien wie .doc, .docx, .docm, .ppt, .pptx, .xls, .xlsx
- Dateiformate, die Sie nicht kennen

Regel: Bei direkt ausführbaren Dateiformaten, öffnen Sie diese nur, wenn Sie diesen Dateianhang genau in dieser Form angefordert haben. Haben Sie diesen Anhang nicht angefordert? Kennen Sie den Absender? Falls Ja, dann fragen Sie beim Absender nach. Benutzen Sie dabei aber keinesfalls die Kontaktdaten aus der E-Mail, sondern greifen Sie auf Ihnen bekannte Kontaktdaten zurück.