Phishing-Prävention

Unter Phishing versteht man cyberkriminelle Angriffe, die darauf abzielen, in den Besitz von Anmeldeinformationen zu gelangen, sowie Anwender zu Aktionen zu veranlassen, die zur Infizierung ihrer Rechner mit Schadsoftware führen. Zu diesem Zweck werden gefälschte, aber vertrauenswürdig aussehende Webseiten und Emails verwendet. Da derartige Angriffe nicht vollständig mit technischen Mitteln verhindert werden können, ist es unbedingt erforderlich, dass alle Hochschulangehörigen sich der Gefahr durch Phishing bewusst sind und auch wissen, wie man Phishing erkennen kann.

1. *Inhalt*: ist der Mail-Text plausibel? Bezieht der Inhalt sich auf aktuelle, bekannte Vorgänge? Passt der Inhalt zur üblichen Kommunikation innerhalb der Hochschule? Einladungen zu Urlaubsreisen, Teilnahme an Gewinnspielen, Privatverkäufe, Suchaufrufe wegen entlaufener Haustiere usw. werden normalerweise nicht kommuniziert. Auch wenn der Angreifer durch vorangegangene Recherche Themen anspricht, die zur persönlichen bzw. beruflichen Situation des Empfängers oder zu Aufgaben und Funktionen der Hochschule passen, so sind die Angaben oft vage und ungenauer, als wenn jemand wirklich mit dem betreffenden Sachverhalt vertraut wäre.
→ Wenn einem also der Inhalt des Schreibens auch nur den geringsten Anlass zum Zweifel gibt, sollte man immer dieses Schreiben genauer prüfen und zwar vor allem dann, wenn ein solches Schreiben Links oder Dateianhänge enthält.

2. *Was kann der Angreifer wissen?* Durch öffentlich frei zugängliche Informationsquellen (Internet im allgemeinen, die Homepage der Hochschule und hier vor allem das Personenverzeichnis, Social Media) erfahren Cyberkriminelle erstaunlich viel. Dieses Wissen ermöglicht ihnen eine spezifische, personalisierte Ansprache, z.B. indem sie Beschäftigten im Einkauf ein Angebot bzgl. Büromaterial unterbreiten. Auch versetzt sie dieses Wissen in die Lage, so zu tun, also wären sie Hochschulangehörige.
→ Vermeiden Sie bei Social-Media-Auftritten detaillierte Angaben zur beruflichen Situation und beschränken Sie den Empfängerkreis auf ein dem Kommunikationszweck entsprechenden Umfang!

3. *Stil und Form:* Ebenso wie der Inhalt muss auch die formale Gestaltung kritisch geprüft werden. Wird man von Personen geduzt, mit denen man per Sie ist (bzw. umgekehrt)? Entspricht der Stil demjenigen, den man von der betreffenden Person kennt bzw. dem Thema angemessen ist? Ist beispielsweise eine offizielle Mitteilung zu organisatorischen Änderungen in einem ungewohnt lockeren Tonfall gehalten oder sieht ein Angebot wirklich so aus, wie ein Angebot aussehen sollte? Sind Anrede und Signatur plausibel? Ein Fremder würde Frau Mustermann nicht mit „Hallo“, sondern mit „Sehr geehrte …“ anreden, unsere EDV-Mitarbeiter würden mit Namen und MIT unterzeichnen und nicht einfach „Ihre Administratoren“.
Die Qualität von Phishing-Mails hat sich im Laufe der Jahre deutlich erhöht. Allerdings finden sich immer noch welche, die in holprigem Deutsch geschrieben sind, was seine Ursache darin hat, dass der Absender im Ausland sitzt und ein automatisches Übersetzungsprogramm verwendet hat. Solche Mails lassen sich sofort als Phishing identifizieren.

4. *Links:* Durch Links kann man zu Seiten geführt werden, die Schadsoftware auf Ihren Rechner herunterladen. Da man nicht vorher testen kann, ob Links gefährlich oder sicher sind, muss man vor einem Klick auf einen Link allergrößte Vorsicht walten lassen.

Wenn man die Maus – ohne zu klicken! – über dem Link positioniert, kann man die Adresse des Links erkennen.
In dem Beispiel „Link1“ lautet die Adresse https://www.bing.com/. Das ist offensichtlich die Adresse der bekannten Suchmaschine und somit droht keine Gefahr.
Link1
Link2
Im Beispiel Link2 ist die Adresse viel komplizierter, ja so kompliziert, dass man, wenn man kein Experte ist, nicht ohne weiteres beurteilen kann, ob man dieser Adresse vertrauen kann: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
In diesem Fall empfiehlt es sich, in einem MS Office-Programm oder im Outlook mit Rechtsklick „Hyperlink bearbeiten“ zu aktivieren und die Basisadresse https://www.bsi.bund.de herauszukopieren und manuell im Browser einzutragen, um zu prüfen, ob diese zu einer vertrauenswürdigen Organisation führt.
Wenn sich dieses Verfahren als zu schwierig oder nicht ausreichend aussagekräftig herausstellen sollte, dann ist es am besten, den Absender der Nachricht zu kontaktieren, um sich bestätigen zu lassen, dass alles seine Ordnung hat.
Vgl. auch unten Punkt 6. Mail-Adresse

5. *Dateianhänge:* Dateianhänge können Schadsoftware enthalten. Alle angehängten Dateien, die in irgendeiner Weise etwas aktiv ausführen, sind extrem gefährlich!
Dies betrifft zum einen Programmdateien, also Dateien, die auf .exe, .bat, .cmd, .com enden und zum anderen Officedateien, die Makros enthalten. Diese enden auf .xlsxm bzw. docxm, wobei das „m“ auf Makro hinweist. Derartige Dateien sollte man am besten gar nicht erst öffnen. Falls doch, darf man auf keinen Fall etwas anklicken, weil dies die Aktivierung der Schadsoftware in Gang setzt. Aber auch gepackte (gezippte) Dateien mit den Endungen .zip oder .rar sind mit Vorsicht zu behandeln, denn Virenscanner sind zumeist nicht in der Lage, diese zu prüfen.
Generell sollte man in angehängten Dateien, denen man nicht zu 100% vertraut, nichts anklikken! Dies gilt auch für Bilder, denn in diesen können unsichtbare Schalter verborgen sein.
Verdächtige Dateien können heruntergeladen und mit dem Virenscanner untersucht werden.
Ein Speichern, ohne vorher die Datei zu öffnen, kann keinen Schaden bewirken.

6. *Mail-Adresse:* Diese ist mit Abstand das wichtigste Beurteilungskriterium, weil hier der Absender Farbe bekennen muss. Die wirkliche Adresse kann man tarnen, aber nicht verbergen. Um dies zu erläutern, soll ein Beispiel aus der Awarenesskampagne vom November 2020 herangezogen werden. Hier wurde ein Übungsmail von der angeblichen Firma Connect Sports mit der Absenderadresse rolf.egert@connect-sports.security-scanned.de verwendet.
Die Adresse ist nicht, wie suggeriert wird, „connect-sports“, was dem Firmennamen entspricht, sondern „security-scanned“, was absolut verdächtig ist. Entscheidend ist immer nur das, was vor dem letzten Punkt steht und nicht das, was Anfang der Gesamtadresse steht.
Das gleiche Schema gilt auch bei Link-Adressen:
http://www.banking.postbank.de/account
http://www.autoscout24.sicher-autos-kaufen.de/angebot 13123
Die erste Adresse ist korrekt, weil vor dem letzten Punkt „Postbank“ genannt wird, die zweite Adresse führt dagegen nicht zu Autoscout24, sondern zur Betrugsseite „sicher-autos-kaufen“.

7. *Nichts preisgeben:* Niemals Authentifizierungsangaben wie user id, Kennwort, PIN außerhalb der üblichen, Ihnen bekannten Anmeldefenster eintragen!

Es wird sehr häufig versucht, unter irgendwelchen Vorwänden (etwas habe sich geändert, es seien technische Probleme aufgetreten oder man brauche dies zur Bestätigung) diese Angaben abzugreifen. Dabei bedienen sich die Angreifer oft täuschend echt aussehender, einen offiziellen Eindruck machender Bildschirmseiten.
Auch wird versucht, indem sich der Angreifer als Administrator ausgibt, auf telephonischem Wege diese Angabe zu erlangen. Dabei wird zumeist versucht, erheblichen Druck aufzubauen („wenn ich nicht sofort ihr Benutzerkonto aktualisieren kann, wird dies oder das passieren"). Lassen Sie sich nicht beeinflussen! Kein wirklicher Administrator wird jemals die Preisgabe Ihres Kennworts verlangen.

8. Welchen Schaden kann Phishing bewirken?
a) Ein Angreifer erhält Zugang zu Ihrer Maildatenbank, wodurch er Kenntnis der Mailadressen Ihrer Kontakte und auch der Betreffzeilen erhält, was ihn in die Lage versetzt, an diese Adressen unter ihrem Namen personalisierte Mails mit Schadsoftware zu schreiben.
b) Alle Daten auf Ihrem PC und Ihren Netzlaufwerken stehen dem Angreifer offen. Diese können eingesehen, manipuliert oder gelöscht werden.
c) Es wird Schadsoftware installiert, wodurch die Funktionsfähigkeit des Rechners beeinträchtigt wird. Der Computer reagiert seltsam, arbeitet langsamer, es öffnen sich ohne Ihr Zutun Fenster, usw.
d) Ihr PC dient als Brückenkopf, von dem aus weitergehende Angriffe aufs Hochschulnetz gestartet werden, wobei sich der Angreifer allmählich Administratorrechte verschafft.
e) Sobald dies geschehen ist, kann auf alle Daten im Netz zugegriffen werden. Besonders gefährlich ist die Implementierung von Ransomware. Durch Ransomware werden alle Daten verschlüsselt, so dass hochschulweit überhaupt keine Computernutzung mehr möglich ist. Die Daten werden erst wieder nach Zahlung eines Lösegelds entschlüsselt. Die PH Ludwigsburg wird sich nicht auf eine solche Erpressung einlassen, zumal es erfahrungsgemäß sehr unsicher ist, ob die Entschlüsselungszusage eingehalten wird. Sollte es zu einem derartigen Vorfall kommen, werden die Daten durch ein älteres, garantiert virenfreies Backup wiederhergestellt. Das bedeutet auch, dass zum einen wegen der Dauer der Problemanalyse und der Wiederherstellung des umfangreichen Datenbestandes die Hochschule mehrere Tage lang offline sein wird und zum anderen aktuelle Daten definitiv verloren sein werden.
f) Zumeist macht sich Schadsoftware nicht sofort nach dem Infizierungsvorgang bemerkbar, weil die Durchforschung des gesamten Netztes und die Erlangung erweiterter Rechte einige Zeit in Anspruch nimmt. Der eigentliche Angriff beginnt erst dann, wenn alle Informationen gesammelt sind. Darum sollten Sie sofort, wenn Sie wegen ungewöhnlichen Verhaltens Ihres Rechners einen Virusbefall befürchten, das MIT benachrichtigen! Je früher man mit Gegenmaßnahmen beginnen kann, desto geringer ist der Schaden.