Spear-Phishing

Kurzfassung / Abstract

Es gibt zwei wesentliche Punkte, an denen Sie einen Phishing-Versuch erkennen können:

- Achten Sie genau auf die **Absender-Adresse** einer Mail und *nicht* auf den vorangesetzten *Absendernamen* - der lässt sich nämlich leicht fälschen!
- Bei Verlinkungen achten Sie genau auf die **Linkadresse**: Verweist diese nicht auf eine mit *https://xyz.hhu.de* beginnende Adresse, handelt es sich um eine Fälschung!

There are two main points by which you can recognize a phishing attempt:

- Pay close attention to the **sender address** of a mail and *not* to the prefixed *sender name* - because this can be easily faked!
- If links are embedded, pay close attention to the **link address**: If it does not refer to an address beginning with *https://xyz.hhu.de*, it is a fake!

Inhalt / Content:

- Was ist Spear-Phishing?
- Woran erkenne ich Spear-Phishing-Mails?
- Umgang mit Spear-Phishing-Mails
- Was tun, falls Sie trotzdem Opfer einer Spear-Phishing-Mail geworden sind?
    - English Version:
- What is Spear-Phishing?
- How can I recognize spear phishing emails?
- Dealing with spear phishing emails
- What to do if you still became a victim of a spear phishing email?

Support

Bei Rückfragen oder Unsicherheiten im Zusammenhang mit Spam oder Phishing-E-Mails kontaktieren Sie bitte:

ZIM-Helpdesk

Tel.: +49 211 81-10111

E-Mail: helpdesk@hhu.de

Gebäude 25.41, Raum 00.53

Servicezeiten: Mo.-Fr. 8.30-18 Uhr

Melden von IT-Sicherheitsvorfällen

CERT (Computer Emergency Response Team)

E-Mail: cert@hhu.de

Weitere Sicherheitshinweise und Informationen

Sicherheitshinweise

Gefälschte Helpdesk-E-Mails

CEO-Fraud-E-Mails

Melden von Spam- und Phishingmails

Blacklisting

Was ist Spear-Phishing?

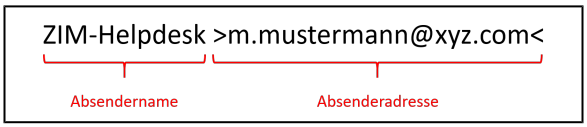
- Wie beim "normalen" Phishing wird beim **Spear-Phishing** versucht, Beschäftigte der Universität zur Preisgabe ihrer Zugangsdaten (Kennung, Passwort) zu verleiten oder Schadsoftware zu downloaden.
- Anders als beim "normalen" Phishing ist der Angriff allerdings **auf die Empfängerin/den Empfänger genau zugeschnitten**: Es wird z.B. auf die genaue berufliche Tätigkeit Bezug genommen, Mails im Namen von Kolleg:innen und Mitarbeiter:innen geschickt oder (falls die Postfächer von Kolleg:innen oder Vorgesetzten kompromittiert wurden) auf eine echte Mailkommunikation aufgebaut.
- Spear-Phishing-Angriffe sind daher besonders gefährlich, da die Kontaktaufnahmeversuche der Täter eine auf den ersten Blick **hohe Authentizität** vorspiegeln.

Woran erkenne ich Spear-Phishing-Mails?

- **Genau auf die Absenderinformation schauen:** Spear-Phishing-Mails geben vor, von einer Ihnen bekannten Person oder Einrichtung zu stammen! Achten Sie bei E-Mails immer genau auf Diskrepanzen zwischen dem *Absendernamen* und der *Absenderadresse*. Wenn Ihnen nur der Absendername angezeigt wird (z.B. auf dem Handy), klicken Sie diesen an und prüfen Sie die Authentizität der Absenderadresse. Wie alle Phishing-Mails werden auch Spear-Phishing-Mails häufig von HHU-externen Postfächern verschickt und sind daher als Fälschungen zu

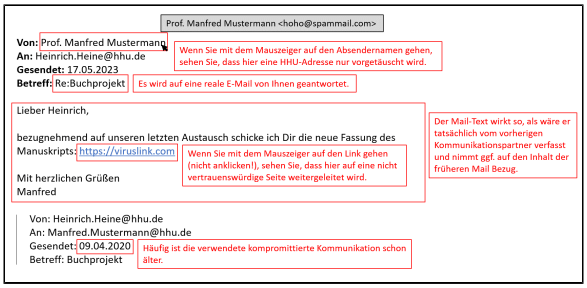
erkennen. Bedenken Sie aber, dass auch HHU-Adressen kompromittiert worden sein können! Wenn Absendername und -adresse voneinander abweichen, ist größte Vorsicht geboten!

Beispiel für das Aussehen einer gefälschten E-Mail-Absenderinformation:



- **Inhalt:** Da Spear-Phishing-Mails in der Regel auf den Empfänger zugeschnitten sind, achten Sie sorgfältig auf Auffälligkeiten im Text, z.B.:
  - Der Text nimmt nicht unmittelbaren Bezug auf die vorhergehende Kommunikation.
  - Die verwendete Kommunikation liegt schon länger zurück (u. U. schon mehrere Jahre).
  - Der Text ist in einer von der vorherigen Kommunikation abweichenden Sprache verfasst.
  - Der Text enthält für den angeblichen Absender ungewöhnliche Rechtschreibe- und Grammatikfehler.
- **Links:** Phishing-Mails enthalten immer einen Link, der entweder hinter einem Fließtext (z.B. "Hier klicken") versteckt ist oder einen Klartext-Namen enthält. Bei nicht auf HHU-Homepages verweisenden Links (die mit *https://xyz.hhu.de* beginnen) ist äußerste Vorsicht geboten. Fragen Sie im Zweifelsfall direkt bei der echten Absenderin/dem Absender nach, ob die Mail von ihr/ihm stammt. "Direkte Nachfrage" heißt in diesem Fall: Nicht als Antwort auf die dubiose Mail, sondern schreiben Sie eine neue Mail an die Ihnen bekannte Adresse der Person oder nehmen Sie auf anderem Weg Kontakt auf.

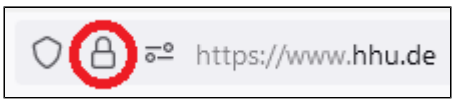
Beispiel für eine Spear-Phishing-E-Mail:



Umgang mit Spear-Phishing-Mails

- **Keine Anhänge öffnen:** Bei per Mail verschickten Anhängen (Dokumente, Bilder, Videos) ist äußerste Vorsicht geboten! Öffnen Sie Anhänge nur, wenn diese Ihnen angekündigt worden /von Ihnen in dieser Form erwartet werden. Aktivieren Sie keine Makros (speziell bei Microsoft Office-Dateien).
- **Keine Links anklicken:** Klicken Sie Links nur an, wenn diese auf vertrauenswürdige Homepages und Dienste verweisen, etwa Seiten der HHU (beginnen stets mit *https://xyz.hhu.de*), die Hochschulcloud Sciebo (beginnt stets mit *https://uniname.sciebo.de*, z.B. *https://uni-duesseldorf.sciebo.de*). Vertrauenswürdige Homepages erkennen Sie in der Regel an dem geschlossenen Schloss-Symbol am Beginn der URL-Zeile.

Sichere Homepages erkennt man am Schlosssymbol in der URL-Zeile:



- **Keine Zugangsdaten preisgeben:** Geben Sie auf Seiten, die nicht eindeutig zur HHU gehören (also mit *https://xyz.hhu.de* beginnen) niemals Ihre Zugangsdaten (Kennung, Passwort) ein!
- **Phishing-Mails melden und in den Spam-Ordner verschieben:** Nutzer:innen des E-Mail-Portals *Roundcube* können auf https://roundcube.hhu.de Spam und Phishing-Mails in den Ordner „Spam“ verschieben und so den Spamfilter trainieren (s. auch https://wiki.hhu.de/x/CoiQAg).
- Nutzer des E-Mail-Portals *Exchange* schicken Spam und Phishing-Mails bitte als Dateianhang (EML-Datei) an die Meldeadresse spamreport@hhu.de. Schieben Sie die betreffende E-Mail hierfür im Webportal https://exchange.hhu.de einfach in eine neue E-Mail (s. hierzu https://wiki.hhu.de/x/CoiQAg, hier unter "Methode 2" schauen).

Was tun, falls Sie trotzdem Opfer einer Spear-Phishing-Mail geworden sind?

Wenn Sie vermuten, dass Unbefugte sich Zugang zu Ihrem Universitätskonto und/oder Computer verschafft haben, ergreifen Sie sofort folgende Maßnahmen:

- **Sofort Passwort ändern:** Ändern Sie sofort auf der Seite https://idm.hhu.de/ Ihr Passwort *oder* informieren Sie den ZIM-Helpdesk, damit dort Ihr Passwort zurückgesetzt wird! Wenn Sie vermuten, dass Ihr Computer gehackt wurde, nutzen Sie für die Änderung des Passworts ein anderes Gerät!
- Falls Ihr Computer mit Schadsoftware infiziert wurde, müssen Sie auch die Passwörter aller von Ihnen genutzten Dienste ändern, auf die Sie von dem betroffenen Computer aus zugegriffen haben (z. B. private E-Mail-Konten, Online-Banking usw.)!
- **Sofort Netzzugang trennen:** Wenn Sie vermuten, dass Unbefugte Zugang zu Ihrem Computer erlangt haben, trennen Sie diesen sofort vom Internetzugang. Wenn Sie über ein LAN-Kabel mit dem Internet verbunden sind, ziehen Sie den LAN-Stecker, falls Sie ein WLAN benutzen, deaktivieren Sie die WLAN-Verbindung Ihres Gerätes!
- **Computer auf Schadsoftware scannen:** Überprüfen Sie den betroffenen Computer in jedem Fall mit einer Virenschutz-Software!
- **Betriebssystem neu installieren:** Wenn möglich, installieren Sie das Betriebssystem des betroffenen Computers neu!
- **Kontakte warnen:** Informieren Sie Ihre E-Mail-Kontakte über die Infektion Ihres Rechners, da für diese Personen jetzt eine erhöhte Gefahr besteht!

English Version:

What is Spear-Phishing?

- As with "normal" phishing, **spear phishing** attempts to trick university employees into revealing their access data (ID, password) or to download malware.
- Unlike "normal" phishing, however, the attack is **precisely tailored to the recipient**: for example, reference is made to the exact professional activity, mails are sent in the name of colleagues and employees, or (if the mailboxes of colleagues or supervisors have been compromised) real mail communication is built upon.
- Spear phishing attacks are therefore particularly dangerous, as the perpetrators' attempts to make contact appear to be **highly authentic** at first glance.

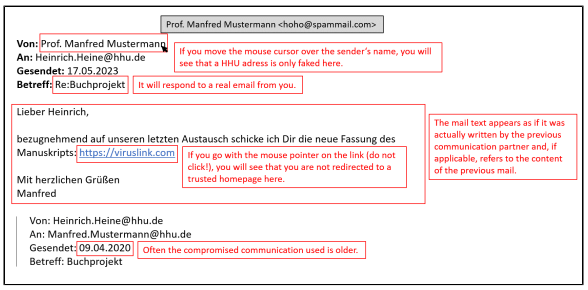
How can I recognize spear phishing emails?

- **Look carefully at the sender information:** Spear phishing e-mails pretend to come from a person or institution you know! Always pay close attention to discrepancies between the sender name and the sender address in e-mails. If you are only shown the sender name (e.g. on your cell phone), click on it and check the authenticity of the sender address. Like all phishing emails, spear phishing emails are often sent from HHU-external mailboxes and are therefore recognizable as fakes. However, keep in mind that HHU addresses may have been compromised as well! If the sender name and address differ from each other, be extremely careful!

Example for a forged sender information:

- **Content:** Since spear phishing e-mails are usually tailored to the recipient, pay careful attention to conspicuous features in the text, e.g.:
  - The text does not make direct reference to the previous communication.
  - The communication used was a long time ago (possibly several years).
  - The text is written in a language that differs from the previous communication.
  - The text contains unusual spelling and grammatical errors for the alleged sender.
- **Links:** Phishing emails always contain a link that is either hidden behind body text (e.g., "click here") or contains a plain text name. Extreme caution is advised with links that do not refer to HHU homepages (which starts with *https://xyz.hhu.de*). If in doubt, ask the real sender directly whether the mail originates from him/her. In this case, "direct inquiry" means not replying to the dubious mail, but writing a new mail to the person's address that you know or contacting them by other means.

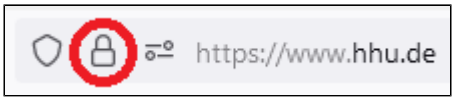
Example for a spear phishing email:



Dealing with spear phishing emails

- **Do not open any attachments:** Extreme caution should be exercised when attachments (documents, images, videos) are sent by e-mail! Only open attachments if they have been announced to you/are expected from you in this form. Do not activate macros (especially for Microsoft Office files).
- **Do not click on links:** Only click on links if they refer to trustworthy homepages and services, such as HHU pages (always starts with *https://xyz.hhu.de*), the university cloud Sciebo (always begins with *https://uniname.sciebo.de*, e.g. *https://uni-duesseldorf.sciebo.de*). You can usually recognize trustworthy homepages by the closed lock symbol at the beginning of the URL line.

Secure Homepages can be recognized by the lock symbol in the URL line:



- **Do not disclose access data:** Never enter your access data (ID, password) on pages that do not clearly belong to HHU (i.e. starting with *https://xyz.hhu.de*)!
- **Report phishing mails and move them to the spam folder:** Users of the Roundcube e-mail portal can move spam and phishing emails to the "Spam" folder at https://roundcube.hhu.de and thus train the spam filter (see also https://wiki.hhu.de/x/CoiQAg).
- Users of the Exchange e-mail portal should send spam and phishing emails as file attachments (EML file) to the reporting address spamreport@hhu.de. To do this, simply move the email in question into a new e-mail in the web portal https://exchange.hhu.de (see https://wiki.hhu.de/x/CoiQAg, look here under "Method 2").

What to do if you still became a victim of a spear phishing email?

If you suspect that unauthorized persons have gained access to your University account and/or computer, take the following actions immediately:

- **Change password immediately:** Immediately change your password on the page https://idm.hhu.de/ *or* inform the ZIM Helpdesk to reset your password there! If you suspect that your computer has been hacked, use another device to change your password!
- If your computer has been infected with malware, you must also change the passwords of all services you use and have accessed from the affected computer (e.g. private email accounts, online banking, etc.)!
- **Disconnect network access immediately:** If you suspect that unauthorized persons have gained access to your computer, disconnect it from the Internet access immediately. If you are connected to the Internet via a LAN cable, disconnect the LAN plug, if you are using a WLAN, deactivate the WLAN connection of your device!
- **Scan computer for malware:** In any case, check the affected computer with antivirus software!
- **Reinstall the operating system:** If possible, reinstall the operating system of the affected computer!
- **Warn contacts:** Inform your e-mail contacts that your computer has been infected, as these people are now at increased risk!