Das Rechenzentrum der Universität Jena bietet einen neuen Service zur Meldung von verdächtigen Phishing-E-Mails an.

Wenn Sie eine E-Mail bekommen und diese als Betrugsversuch erkannt haben oder sie sich wegen eines möglichen Phishing-Versuchs unsicher sind, dann sollten Sie weder auf Links klicken noch Dateianhänge öffnen oder auf die E-Mail antworten. Mit einer Antwort auf Phishing-E-Mails bestätigen Sie die Existenz und Aktivität Ihres E-Mail-Kontos.

Fragen Sie immer nach! Auch bei bekannten und vertrauten Personen!

Leiten Sie im Verdachtsfall solche E-Mails an phishing@uni-jena.de weiter.

QUELLEN:

Spam, Phishing & Co - Phishing

www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html

KONTAKT

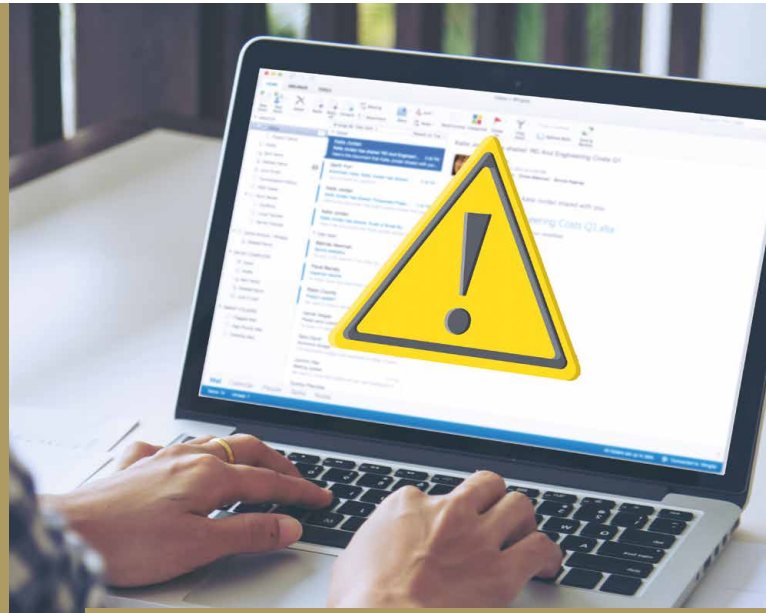
Friedrich-Schiller-Universität Jena
Universitätsrechenzentrum
IT-Service-Zentrum

Telefon: +49 3641 9-404777
Fax: +49 3641 9-404666
E-Mail: phishing@uni-jena.de

Herausgeber: Universitätsrechenzentrum
Fotos: Kay Ludwig | freepik.com | pexel.com/Polina Zimmerman
Layout: Sandra Kraut, nach einer Vorlage der Abteilung Hochschulkommunikation

www.uni-jena.de/urz

FRIEDRICH-SCHILLER-
UNIVERSITÄT
JENA Universitätsrechenzentrum



PHISHING-E-MAILS

Verhaltensweisen zum Umgang

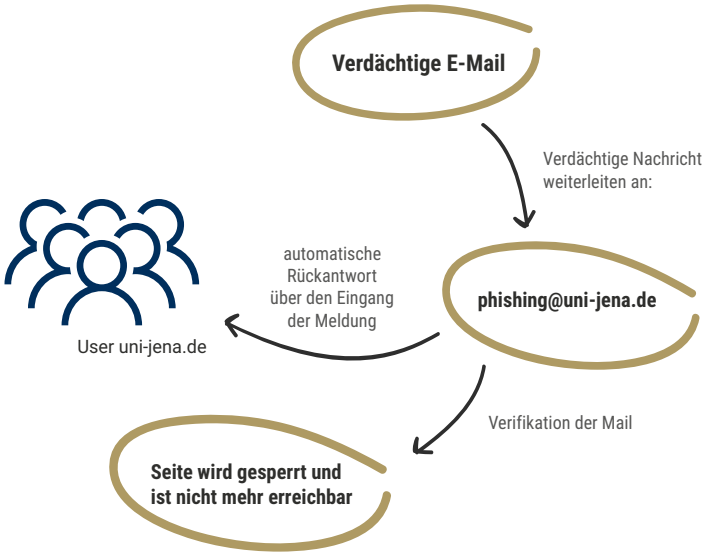
WAS IST PHISHING?

Das Wort setzt sich aus **»Password«** und **»fishing«** zusammen, zu Deutsch **»nach Passwörtern angeln«**.

Formal gesehen passiert ein solcher Angriff in zwei Etappen, die manchmal auch einzeln auftreten:

1. Da ist zum einen die E-Mail, die ein Vertrauensverhältnis ausnutzt und entweder auf eine bösartige Internetseite lockt oder Computerschädlinge im Schlepptau hat. Diese E-Mails sind heute übrigens oft perfekt formuliert.

2. Zum anderen gibt es die Nachahmung von Teilen oder einer gesamten vertrauten Webseite, auch „Spoofing“ („Verschleierung“) genannt. Hier geschieht der eigentliche Betrug, indem die Angreifer einen getäuschten Nutzer zur Preisgabe vertraulicher Daten verleiten, die dann missbraucht werden.



WORAN KANN MAN PHISHING-E-MAILS ERKENNEN?

Im schlimmsten Fall erkennen Sie das nicht. Beispiele finden Sie beim Bundesamt für Sicherheit in der Informationstechnik (siehe Quelle).

» Die Absenderadressen sind zumeist gefälscht. Die Erkennung des gefälschten Absenders ist nur über die Header-Auswertung möglich.

» Die Anrede ist meistens unpersönlich gehalten.

» Dringender Handlungsbedarf wird signalisiert („sofort, sonst…“) und Drohungen kommen zum Einsatz.

» Vertrauliche Daten (wie zum Beispiel PINs und TANs) werden abgefragt, etwa in einem Formular innerhalb der E-Mail.

» Die E-Mails enthalten Links oder Formulare, die vom Empfänger verfolgt beziehungsweise geöffnet werden sollen.

» Die Nachrichten sind manchmal (aber nicht immer!) in schlechtem Deutsch verfasst.

» Die E-Mails enthalten manchmal (aber nicht immer) kyrillische Buchstaben oder falsch aufgelöste bzw. fehlende Umlaute (z. B. nur „a“ statt „ä“ beziehungsweise „ae“).

Ich habe versehentlich meinen Nutzernamen und mein Passwort wie aufgefordert eingegeben. Was soll ich jetzt tun?

Ändern Sie umgehend Ihr Passwort! Gehen Sie auf https://portal.uni-jena.de.

Wenn Sie zudem dieses Passwort auch bei IT-Diensten außerhalb der Universität (PayPal, iTunes, Ebay, Amazon etc.) verwenden, ändern Sie unbedingt auch dort Ihr Passwort. Verwenden Sie für jedes Portal ein anderes Passwort!

Ich habe mich immer korrekt verhalten und trotzdem keinen Zugriff mehr auf mein E-Mail-Konto. Was kann ich tun?

E-Mail-Konten werden in Verdachtsfällen automatisiert gesperrt. Das Entsperren ist durch das IT-Servicezentrum des Universitätsrechenzentrums möglich und setzt eine vorherige Passwortänderung voraus (E-Mail: itservice@uni-jena.de).

Wie kann es dazu kommen, dass solche E-Mails von vermeintlichen E-Mail-Adressen der Universität mit bekannten und vertrauten Inhalten an mich geschickt werden?

Wenn Mitarbeiter bereits Ihre Zugangsdaten bei Aufforderung eingegeben haben, besitzen die Angreifer Zugriff auf das E-Mail-Konto und somit auch auf das globale Adressbuch der FSU. Die Angreifer nutzen dann E-Mail-Adressen und Inhalte der E-Mails des kompromittierten Kontos für weitere Angriffe. Das lässt die Phishing-E-Mails täuschend echt aussehen und erhöht die Erfolgswahrscheinlichkeit der Angreifer.

Teilen Sie bitte diese Information dem IT-Servicezentrum mit.