Was ist Phishing?

Information für Studierende
Stand: Jänner 2020

Vorwort

Liebe Studierende! Lieber Studierender!

Wir wissen, dass in den allermeisten Fällen auf Phishing

1. aus Pflichtbewusstsein
2. in Stresssituationen, z.B. vor Prüfungen
3. aus Unwissenheit

falsch reagiert wird.

Daher bitten wir auch um Verständnis, dass zum Schutz Ihrer Daten

1. Ihr Account wegen Gefahr im Verzug gesperrt werden muss, auch wenn Sie uns mitgeteilt haben, dass Sie Ihr Passwort bereits geändert haben.
2. wir ggf. zur Aufklärung des Vorfalls und der Verhinderung zukünftiger Probleme ein Awareness-Gespräch führen müssen.

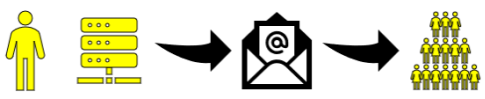
Was ist Phishing?

Unter Phishing versteht man im Wesentlichen

1. die Vorspiegelung falscher Tatsachen in betrügerischer Absicht.
2. mit dem Ziel unberechtigten Zugang zu erlangen.
3. aus diesem unberechtigten Zugang generiert der Angreifer dann seinen Vorteil.

Beispiele

Vorspiegeln falscher Tatsachen



Eine E-Mail von einer Person der Administration mit der Aufforderung auf einen (gefälschten) Link zu klicken und dort die persönlichen Zugangsdaten einzugeben, wird an eine große Zahl an Personen einer Organisation geschickt.

In Wirklichkeit wurde der Bediensteten-Account missbraucht und gezielt die betrügerische E-Mail gestreut.

Erlangen eines unberechtigten Zugangs

Ein Teil der mit der Falschmeldung versorgten Personen gibt die persönlichen Zugangsdaten auf dem Server der Kriminellen ein.

Betrügerische Vorteile

Auf den Servern der Kriminellen (rot) landen die Accountdaten. Die Kriminellen verwenden nun die sehr leistungsfähige E-Mail Infrastruktur um über die gephishten Accountdaten weitere Organisationen anzugreifen oder bezahlten Spam zu verschicken.

Wie erkenne ich Phishing?

Absender

Da Phishing E-Mails fast immer von gestohlenen (gephishten) Accounts verschickt werden und die Opfer meist nicht sehr aufmerksam sind, machen sich die Kriminellen oft nicht einmal die Mühe, die Absenderadresse zu fälschen. Daher erkennt man eine Phishing E-Mail schon oft daran, dass die Absender-adresse **nicht von uni-graz.at** kommt. Aber ACHTUNG ein „echter" Absender ist **kein Echtheitskriterium**!

Adressat

Ist kein Adressat oder ein anderer als deine E-Mail Adresse vorhanden, wurde die Mail als BCC (Blind Carbon Copy) an deine Adresse verschickt. Das macht neugierig und muss die Alarmglocken schrillen lassen!

Mailtext – Psychologische Komponente

Ist der Mailtext irgendwie bedrohlich (negativ) *„Wenn sie das nicht machen, dann …"* oder euphorisch (positiv) *„Sie haben gewonnen …"* so ist jedenfalls Skepsis angebracht.

Mailtext – Form

Enthält der Mailtext viele Rechtschreibfehler, schlechte Grammatik oder scheint aus einer Übersetzungssoftware zu kommen, ist ebenfalls Vorsicht geboten. Passt auch Umgangston oder -formen nicht zur vermuteten Absenderadresse sind das auch Anzeichen zur Vorsicht.

Mailtext – Links / Verweise

Sind Links im Mailtext enthalten, so überprüfen Sie mit einem Mouse Over (mit der Maus zum Linken fahren und warten bis im Pop-Up der Link angezeigt wird) den Link. Passt der Domainname nicht zur Uni Graz oder schlägt aus dem Kontext, dann ist ebenfalls Skepsis angebracht.

Mail-Anhänge

Anhänge können neben betrügerischem Inhalt auch Malware enthalten. Wenn ein Anhang nicht im Kommunikationskontext mit dem Gegenüber kommt, so sollten Sie beim Öffnen größte Vorsicht walten lassen (Malware Scanner aktualisieren, keine Makros in Office Dokumenten starten). Oft ist es besser auf das Öffnen gänzlich zu verzichten oder vorher über einen alternativen Kommunikations-kanal die Echtheit des Anhangs bestätigen lassen.

Alternativer Kommunikationskanal

Haben Sie Zweifel an einer E-Mail, so verwenden Sie wenn möglich einen alternativen Kommunikationskanal (Telefon, Chat, persönlich etc) zur vermuteten Absenderadresse. Der Servicedesk/Infopoint der uniIT unterstützt dich ebenfalls, bei der Klärung derartiger Zweifel.