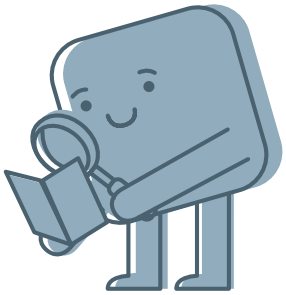
Phishing

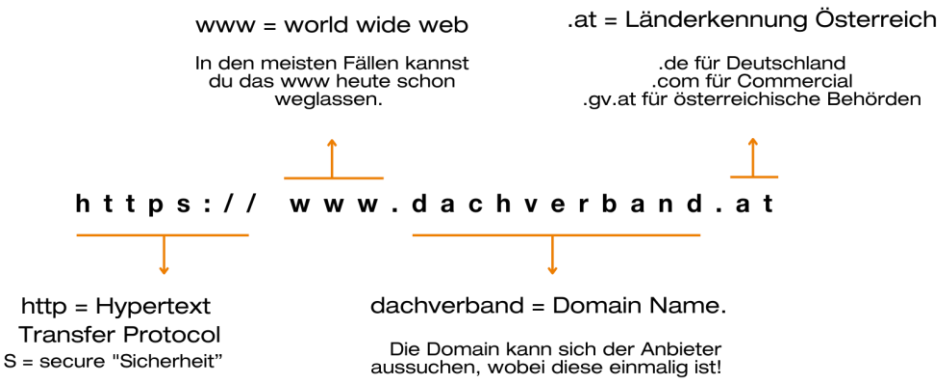


Phishing, der Betrug, um an Konto- und Zugangsdaten oder Geld zu gelangen, passiert auf verschiedene Arten. Die häufigsten Arten sind:

- Per E-Mail (Phishing = Password + Fishing)
- Per SMS (Smishing = SMS und Phishing)
- Per Anruf (Vishing = Voice Vishing)
- Voice Cloning – ein Phishing Anruf mit einer nachgemachten Stimme
- Spear Phishing – Phishing bei dem das Opfer zuerst über Social Media ausgeforscht wird.
- CEO Fraud – eine Phishing Attacke, bei der sich Betrüger als dein Geschäftsführer ausgeben.

Wichtige Faktoren, um Phishing zu erkennen:

1) Die Anrede: Meistens allgemein gehalten. Bei Spear Phishing auch persönlich. Unternehmen, bei denen du ein Benutzerkonto hast, werden dich immer persönlich ansprechen!
2) Die Absender-Adresse: hinter dem Anzeigenamen des Absenders kann alles stehen. Schaue genau, ob der Absender auch zum Inhalt der Nachricht passt (zum Beispiel: wird deine Bank keine Nachricht von gmail.com senden!)
3) Link: Fahre mit der Maus über den Link, ohne diesen anzuklicken. Passt die angegebene URL zum Absender beziehungsweise der vorgetäuschten Firma? Logge dich niemals über einen verdächtigen Link in ein Online Portal ein!

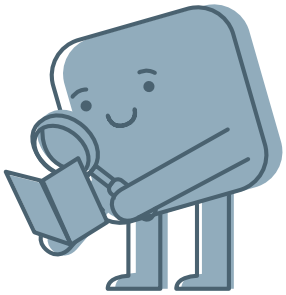


4) Dateianhänge: öffne keine Dateianhänge in den Formaten .exe oder .zip. Sei ebenso vorsichtig bei allen anderen Formaten (.bat, .xslm, .docm, …).
5) Rechtschreib- und Grammatikfehler: Phishing E-Mails sind häufig in fehlerhafter Sprache verfasst.
6) Gefühle: Angreifende versuchen unsere menschlichen Gefühle zu adressieren. Wird Druck erzeugt in dieser E-Mail? Wird zum Beispiel dein Konto sonst gesperrt? Dann handelt es sich wahrscheinlich um eine Phishing Nachricht.

Verdacht auf Phishing? - Bewahre Ruhe!

- Klicke keine Links an und lade keine Dateianhänge herunter, wenn der Verdacht auf Phishing besteht!
- Halte Rücksprache mit deiner Führungskraft, wenn du dir unsicher bist.
- Informiere umgehend deine IT-Abteilung, über den Vorfall (insbesondere dann, wenn du versehentlich auf einen Link geklickt hast!)

E-Mail-Sicherheit



Risikofaktoren im Umgang mit E-Mails:

1) Gefälschte E-Mails wie zum Beispiel Phishing.
2) E-Mail Anhänge. Diese können Viren oder schadhafte Software beinhalten.
3) Sensible Daten, wie Gesundheitsdaten, können als Anhang gesendet, leicht in die falschen Hände gelangen.
4) Empfänger: schnell vertippt und schon bekommt jemand Fremdes die Nachricht.

Senden:

1) Halte den Empfängerkreis so klein wie möglich.
2) Achte darauf, dass nur Personen die Nachricht erhalten, die diese auch erhalten dürfen und für die der Inhalt relevant ist.
3) Vertrauliche Daten solltest du nicht per E-Mail versenden.
4) Sende Dateien über das Datenaustausch System deiner Organisation.

Empfangen: Achte auf die Phishing Faktoren!

1) Versuche immer den Absender der E-Mail zu identifizieren.
2) Prüfe den Inhalt auf seine Echtheit!
3) Sei im Umgang mit Dateianhängen besonders vorsichtig!

Weiterleiten:

Beachte beim Weiterleiten von E-Mails auf den Inhalt sowie den Empfängerkreis. Es werden nicht nur alle E-Mail-Adressen des bisherigen Schriftverkehrs sondern auch der gesamte Inhalt der Konversation mitgesendet! Überlege vor dem Weiterleiten daher immer, ob die hinzugefügte Person auch berechtigt ist, die beinhalteten Informationen zu empfangen!

Halte dich beim Senden und Empfangen von E-Mails immer an die Richtlinien deiner Organisation!

DACHVERBAND
WIENER SOZIALEINRICHTUNGEN