Die folgenden Schulungseinheiten wurden innerhalb des vom **Bundesministerium für Wirtschaft und Energie** im Rahmen der **Initiative IT-Sicherheit in der Wirtschaft** geförderten Projekts **KMU Aware** entwickelt.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

KMU AWARE
AWARENESS IM MITTELSTAND

IT-Sicherheit
IN DER WIRTSCHAFT

Modul 1: Einführung in das Thema „Phishing und andere gefährliche Nachrichten“

Aufbau

1. Erklärung, was gefährliche Inhalte sind
2. Erklärung, was mögliche Konsequenzen sind
3. Erklärung, wie Betrüger vorgehen

Betrüger bauen die **gefährlichen Inhalte** auf unterschiedliche Weise in betrügerische Nachrichten ein. Weit verbreitet sind die folgenden Nachrichtenformate:

(1) Die Nachrichten fordern Sie auf zu antworten und dabei verschiedene sensible Daten wie Passwörter und Kreditkartendaten anzugeben. Ziel der Betrüger ist es hierbei an die geforderten Informationen zu gelangen.

(2) Die Nachrichten fordern Sie auf, Überweisungen z.B. an vermeintliche Geschäftspartner oder Anrufe z.B. an vermeintliche Geschäftspartner zu tätigen.

(3) Die Nachrichten enthalten einen oder mehrere betrügerische Links. Ziel der Betrüger ist es hierbei, dass Sie auf einen der Links klicken. Diese Links leiten Sie dann z.B. zu einer betrügerischen aber authentisch aussehenden Webseite, bei der Sie sich einloggen sollen, oder zu einer Webseite, die Ihnen Schadsoftware installiert. Die Links müssen Sie nicht einmal zur direkten Eingabe von Daten auffordern; bereits Nachrichten, die Sie lediglich auf Informationen hinweisen, können gefährliche Links enthalten.

(4) Die Nachrichten enthalten eine gefährliche Datei (z.B. einen Anhang in einer E-Mail). Ziel der Betrüger ist es hierbei, dass Sie den Anhang öffnen bzw. ausführen.

Betrüger können mehrere dieser Ziele gleichzeitig verfolgen und Nachrichtenformate kombinieren. So könnten Sie z.B. aufgefordert werden, entweder auf einen Link zu klicken oder persönliche Daten als Antwort an den Absender zu schicken.

Oft werden die Nachrichtenformate (1) und (3) auch als Phishing bezeichnet.

Die **Konsequenzen**, die durch das Klicken gefährlicher Links oder das Öffnen eines gefährlichen Anhangs entstehen können, sind gravierend.

So können Betrüger mithilfe von Schadsoftware – z.B. Viren und Trojaner – je nach Ausprägung der Software unterschiedlichen Schaden anrichten. Zum Beispiel könnte Schadsoftware

- alle von Ihnen durchgeführten Aktionen an Ihrem Gerät ausspähen, z.B. Passworteingaben. Diese Informationen können sowohl zum Identitätsdiebstahl genutzt werden als auch, um Sie oder Ihr Unternehmen zu erpressen.
- eigene Aktionen an Ihrem Gerät durchführen, z.B. private Fotos oder andere Dateien kopieren, verändern und verschicken, Kamera und / oder Mikrophon einschalten und mitlesen. Diese Daten können dann z.B. genutzt werden, um Sie zu erpressen.
- die Funktionstüchtigkeit so einschränken, dass Sie Ihr Gerät nicht mehr nutzen können. Die Betrüger fordern Sie dann z.B. zur Zahlung eines gewissen Betrages auf, um Ihr Gerät wieder nutzbar zu machen.

Betrüger können durch das Abgreifen von Zugangsdaten (über Schadsoftware oder nach der Benutzereingabe von Zugangsdaten auf einer betrügerischen Webseite oder durch das Beantworten von Nachrichten) zum Beispiel

- in Ihrem Namen mit Kollegen, Vorgesetzten, Verwandten, Freunden, Bekannten über den entsprechenden Dienst kommunizieren.
- in Ihrem Namen einkaufen sowie Buchungen und Überweisungen tätigen (z.B. bei Paypal).
- erheblich in Ihre Privatsphäre eingreifen, indem sie alle Informationen über Sie bei dem Anbieter sehen und / oder lesen, z.B. gespeicherte Fotos, Kontaktinformationen Ihrer Kommunikationspartner, Kommunikationsverläufe und Nachrichten (E-Mails usw.). Derartige Daten können dann z.B. zur Erpressung genutzt werden, wenn Sie nicht einer bestimmten Zahlung nachkommen

Betrüger erhalten direkt Geld von Ihnen, wenn Sie das Geld wie gefordert auf das in der Nachricht angegebene Konto überweisen oder die kostenpflichtige Telefonnummer aus der Nachricht anrufen.

Betrüger **geben sich in ihren Nachrichten als Anbieter oder Einzelperson aus**. Sie schicken Ihnen Nachrichten,

- in denen sie vorgeben, ein Ihnen bekannter und vertrauter Anbieter zu sein. So geben sie z.B. vor Ihre Bank, Amazon, PayPal, DHL, Ebay, Microsoft oder SAP zu sein.

- in denen sie vorgeben, eine Ihnen bekannte Person zu sein.

- in denen sie zwar nicht vorgeben ein Ihnen bekannter und vertrauter Anbieter oder eine Ihnen bekannte Person zu sein. Sie versuchen aber durch den Inhalt der Nachrichten Aufmerksamkeit mit attraktiven Versprechungen und Verlockungen zu erzeugen. So wird Ihnen z.B. ein Gewinn, ein Geschäft mit hohen Einkünften oder eine vielversprechende Information in Aussicht gestellt. Oder es wird eine angeblich offene Rechnung geschickt, oder Interesse an Ihnen und / oder dem Unternehmen signalisiert, z.B. in Form einer (Initiativ-)Bewerbung.

Weiterführende Hinweise: Beachten Sie, dass die Inhalte der Nachrichten sehr unterschiedlich und auf den Kontext angepasst sein können. Dabei greifen Betrüger häufiger auf öffentlich zur Verfügung stehende Informationen zurück, z.B. Informationen, die Sie in sozialen Netzwerken über sich preisgeben, oder Informationen, die das Unternehmen auf der Unternehmenswebseite veröffentlicht. Die Risiken, die mit dem Veröffentlichen persönlicher Informationen einhergehen, erhöhen sich oftmals immens durch das Verknüpfen von Informationen verschiedener Quellen.

Betrüger verfolgen eine der folgenden Strategien bei der Auswahl der **Empfänger** (und damit potentiellen Opfer):

- Sie haben es genau auf Sie und / oder Ihr Unternehmen abgesehen. Sie haben es genau auf Sie und/oder Ihr Unternehmen abgesehen. Beachten Sie, dass nicht nur die direkte Preisgabe persönlicher Informationen in sozialen Netzwerken oder auf Webseiten, sondern auch Verbindungen zu Personen, die einer Interessengruppe zugehören, Rückschlüsse über Ihre Interessen zulassen und Sie somit für Betrugsversuche anfällig scheinen lassen.
- Sie haben es nicht auf konkrete Einzelpersonen abgesehen, sondern verschicken die Nachrichten an Millionen von Kontakten.

Ihre Kontaktdaten haben die Betrüger entweder von Ihrer Webseite oder der Webseite des Unternehmens, bei dem Sie arbeiten, aus sozialen Netzwerken, von nicht-vertrauenswürdigen Webseiten, bei denen Sie diese angegeben haben, oder auch von einer vertrauenswürdigen Webseite, die gehackt wurde.

Es ist für beide Strategien egal wie alt Sie sind, welche Position Sie im Unternehmen haben und welches Einkommen oder Vermögen Sie haben. Betrug um kleine Beträge, dafür aber in der Masse, sind auch ein äußerst lukratives Geschäft.

Betrüger verschicken Nachrichten **mehrfach und zu beliebigen Zeitpunkten**,

- da das Erstellen und Verschicken von betrügerischen Nachrichten sehr einfach, ohne tiefgehendes technisches Wissen und ohne großen zeitlichen Aufwand möglich ist. Sie nutzen dabei z.B. Tools, die frei im Internet verfügbar sind.
- da sich so die Wahrscheinlichkeit erhöht, dass Sie zu einem der gewählten Zeitpunkte eine Nachricht des (vermeintlichen) Absenders für möglich halten oder gar erwarten (weil Sie z.B. gerade bei Amazon etwas bestellt haben).

Durch dieses Vorgehen steigt die zu erwartende Ausbeute der Betrüger.

Die Gefahren des Informationsmissbrauchs können nicht nur ausschließlich Sie betreffen, sondern gerade auch Ihr nahes Umfeld, z.B. Kollegen, Vorgesetzte, Familie und Freunde.

Betrüger nutzen **verschiedene Dienste**, um Ihnen Nachrichten zu schicken. Hierzu gehören z.B.:

- E-Mail

- Messenger wie Skype und WhatsApp, Instagram und Snapchat

- soziale und berufliche Netzwerke wie Facebook, Google+, XING und LinkedIn

- SMS, MMS

Betrüger richten ihre Strategien darauf aus, verfügbare und von Ihnen und / oder Ihrem Unternehmen eingesetzte **technische Schutzmaßnahmen** wie z.B. Spam-Filter, Virenscanner und Firewalls zu umgehen. Daher sind technische Schutzmaßnahmen leider nicht immer gut genug, um alle betrügerischen Nachrichten unmittelbar als solche zu erkennen.

Die Strategien der Betrüger sind den technischen Schutzmaßnahmen häufig einen Schritt voraus, da technische Schutzmaßnahmen aufwendig entwickelt und getestet werden müssen.

Die verschiedenen technischen Schutzmaßnahmen reduzieren die Risiken, die mit betrügerischen Nachrichten einhergehen, können Sie und / oder Ihr Unternehmen jedoch nicht vollständig schützen. Daher ist es sehr wichtig, dass jeder – auch Sie – solche betrügerische Nachrichten erkennen kann.

Nachdem Sie nun das Vorgehen der Internetbetrüger sowie die daraus entstehenden Konsequenzen kennen gelernt haben, erklären wir Ihnen in den folgenden drei Modulen, wie Sie zwischen betrügerischen und nicht betrügerischen Nachrichten unterscheiden können.

Eine wichtige Information vorweg: Nachrichten, die Sie als betrügerische Nachrichten haben, sollten Sie direkt löschen.