Viele tauchen zunächst nur in englischer Sprache auf und werden später von einer Person ins Deutsche übersetzt und weitergeleitet. Das Gleiche gilt auch für Kettenbriefe. Ziel ist es, technisch nicht versierte Computernutzer/innen zu verunsichern, zu einer bestimmten Reaktion zu bewegen oder gar in Panik zu versetzen. Hoaxes und Kettenbriefe fallen in die Kategorie der Spams.

Erkennen Sie eine Nachricht als Hoax, führen Sie folgende Schritte durch:

1. **Leiten Sie die Nachricht nicht weiter,** um an dieser Stelle die Wanderschaft des Hoax zu unterbrechen.
2. **Informieren Sie die Senderin/den Sender** der Nachricht, dass es sich um eine Falschmeldung gehandelt hat.
3. Wenn Sie nicht sicher sind, ob eine Nachricht ein Hoax ist, **recherchieren Sie in Datenbanken von Antivirusunternehmen** oder über anerkannte Institutionen oder in der Fachliteratur, ob das Virus dort bekannt ist oder bereits als Hoax registriert wurde (**www.hoax-info.de**).
4. **Löschen Sie keine Datei** auf dem PC wegen eines derartigen E-Mails.

Beispiele: Kettenbrief

SEHR WICHTIG !!!!!!!!!

An einer Tankstelle, tankte eine Frau ihr Auto,da wurde Sie von einem Mann als Maler bekleidet,angesprochen,ob Er ihr helfen könne.
Sie verneinte... Er bot ihr seine Visitenkarte an,falls Sie einen Maler bräuchte. Nach einem hinundher, ...um ihn loszuwerden nahm Sie die Visitenkarte an und der dubiose Herr stieg in einem Auto ein das von einem zweiten Mann gelenkt wurde, und Sie fuhren davon. Nachdem Sie losfuhr fühlte Sie sich immer berauschter und hatte mühe zu atmen. Sie öffnete das Fenster und bemerkte gleichzeitig das dieser komische Geruch von Ihrer Hand stammt, mit der Sie die Visitenkarte entgegen nahm !!
Die 2 Männer verfolgten Sie. Da es ihr sichtlich immer schlechter ging fuhr sie auf den nächsten Parkplatz,stoppte, begann wie wild zu Huppen und schrie um Hilfe. Die 2 verfolger fluchteten,ihr ging es aber immer schlechter.
DIE VISITENKARTE WURDE IN EINE FLÜSSIGKEIT DROGE GETRÄNKT, die BURUNDANGA HEISST,sie wird von Kriminellen verwendet um Leute zu Berauben oder Vergewaltigen !!!

Diese flüssige Droge kann über verschiedensten Arten von Papieren an jeden übertragen werden und somit diese Person ausser gefecht setzen.
Diese Substanz ist viel viel schädlicher und wirksamer als jegliche ursprüngliche Droge oder Schlafmittel.
Also,nehmt keine Visitenkarten oder Ähnliches von wildfremden an !!!!
Ähnliche Masche, Sie werfen eine Visitenkarte in den Briefkasten und warten im Auto bis jemand reintappt und dann schlagen Sie zu !!!
Andere Möglichkeit sind die Typen die einem angeblich das Auto für den Export abkaufen wollen und einem die VK bei der Scheibe der Fahrerseite befestigen !!!

SEID VORSICHTIG und warnt soviel Leute wie möglich.

Originaltext

Aufgrund eines Hoax müssen keine Dateien von Ihrem PC gelöscht werden!

Hoaxes sind Falschmeldungen. Man kann sie mit der sogenannten Zeitungsente (Falschmeldung in Zeitungen) vergleichen.

Haben Sie auch schon einmal einen Kettenbrief per E-Mail erhalten? Wie haben Sie darauf reagiert? Wie hätten Sie im Nachhinein betrachtet darauf reagieren sollen?

Nähere Informationen zu Hoaxes finden Sie unter www.hoax-info.de

1.2.4 Scams

Anders als Hoaxes und Kettenbriefe zielen Scams darauf ab, den Empfängerinnen und Empfängern finanziellen Schaden zuzufügen.

Beim Scamming kontaktieren Kriminelle die potenziellen Opfer über soziale Netzwerke oder per E-Mail. Dabei wird beispielsweise ein hohes Erbe eines unbekannten Verwandten versprochen. Eine gängige Praktik ist z. B. auch das Inserieren von günstigen Wohnungen, die es gar nicht gibt, oder der Beginn einer Internet-Romanze – man spricht von Immobilien- bzw. Love-Scamming.

Besonders ältere und einsame Menschen werden Opfer von Scamming.

Ablauf von Scamming

Beispiel: Immobilien-Scamming

Sarah sucht eine günstige Wohnung. Sie findet etwas Passendes: tolle Lage, möbliert und eine unschlagbar günstige Miete. Sarah schreibt ein Mail und erhält rasch eine Antwort – auf Englisch. Der Eigentümer lebt im Ausland, die Wohnung hat er für die Tochter zum Studieren gekauft und möchte sie nach deren Abschluss vermieten. Aus gesundheitlichen Gründen kann er leider nicht nach Österreich kommen, aber die Wohnung kann besichtigt werden. Sarah möchte einen Besichtigungstermin vereinbaren. Die Antwort kommt wieder prompt: Sarah soll eine Kaution von 1.500 Euro überweisen, damit sie den Code für die Schlüsselbox und den Mietvertrag bekommt. Wenn sie die Wohnung nicht will, erhält sie ihr Geld zurück. Sarah wird stutzig: Mietvertrag? Kaution?

Was hätten Sie an Sarahs Stelle gemacht? Haben Sie schon einmal ein Scam erhalten, z. B. über eine angebliche Erbschaft?

So schützen Sie sich vor Scams!

- Vertrauen Sie keinen fremden Personen im Internet.
- Zahlen Sie niemals Geld an unbekannte Personen.
- Bewahren Sie alle Nachrichten auf. Im Betrugsfall dienen sie als Beweise für die Polizei.

Übung

- **Informationsblatt erstellen**
  Erstellen Sie für Ihre Mitschülerinnen und Mitschüler ein übersichtliches Handout, auf dem Sie Spams, Hoaxes, Kettenbriefe und Scams vorstellen. Folgendes soll enthalten sein:
  - Definition der Begriffe mit jeweils einem Beispiel (recherchieren Sie online).
  - Arten von Kettenbriefen: Gewinnspiele, sinnlose E-Petitionen, Glücksbriefe, Tränendrüsenbriefe, Urban Legends. Recherchieren Sie zu den Varianten und stellen Sie je ein Beispiel vor.
  - Tipps, wie und ob man auf die Nachrichten reagieren soll.

1.2.5 Spyware

Unter Spyware versteht man Programme, die immer dann, wenn Anwenderinnen und Anwender online sind, Informationen über den Rechner, die Surfgewohnheiten und ähnliche Informationen in das Netzwerk senden und damit in die Privatsphäre der Anwenderinnen und Anwender eindringen. Zumeist wissen diese nichts über diese Vorgänge.

Die Empfängerinnen und Empfänger der Informationen können die Gewohnheiten der Anwenderinnen und Anwender beim Surfen und beim Einkaufen nachvollziehen. Den finanziellen Hintergrund für Spyware stellen **große Anzeigennetzwerke (Adware Networks)** bereit. Sie zahlen den Programmiererinnen/Programmierern bzw. den Herstellern von Utilities und Spielen, in denen entsprechende Spyware integriert wurde, 10 bis 20 US-Cent pro Download.

Mit den Daten, die sie über die Spyware bekommen, können diese Netzwerke potenziellen Kundinnen/Kunden treffsicher und ungefragt Anzeigen auf den Bildschirm spielen.

www.safer-networking.org

1.2.6 Phishing – Pharming

Phishing

Phishing setzt sich aus den Begriffen „Password" und „Fishing" zusammen. Mithilfe gefälschter E-Mails wird versucht, an vertrauliche Kundendaten zu gelangen. Diese E-Mails fordern die Empfängerinnen bzw. Empfänger zur Aktualisierung ihrer persönlichen Daten auf.

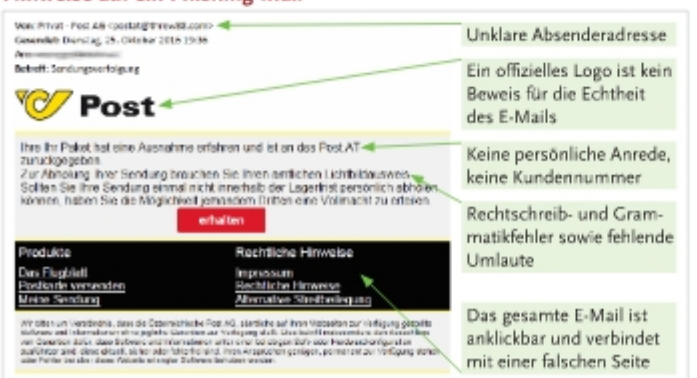
Die Benutzerinnen bzw. Benutzer werden mit Links auf scheinbar seriöse Unternehmenswebsite gelockt, die dem Log-in des jeweiligen Dienstleisters täuschend ähnlich sind.

Zum Beispiel fordern solche Phishing-Mails als Kreditinstitut getarnt die Empfängerinnen bzw. Empfänger auf, ihre persönlichen Daten, Passwörter oder PIN-Codes zu aktualisieren. Die gefälschten Formulare sehen den echten täuschend ähnlich. Einmal im Besitz der sensiblen Daten, haben die Betrügerinnen/Betrüger ungehindert Zugang zu den Konten.

Die Bekämpfung von Phishing ist viel schwieriger als die von Spams, weil der Inhalt der E-Mails so täuschend echt wirkt. Der beste Schutz ist Wachsamkeit.

Ihr Kreditinstitut wird Sie niemals per E-Mail dazu auffordern, Ihre persönlichen Codes und Daten über eine Webseite zu aktualisieren.

Hinweise auf ein Phishing-Mail



Notizen

Es gibt in Phishing-Mails keine Möglichkeit, die eigene Adresse aus dem Verteiler zu löschen („unsubscribe"). Kreditinstitute, Versicherungen etc. würden ihre Kunden nie per E-Mail auffordern, sich auf eine Website einzuloggen und persönliche Daten, z. B. die Kontonummer und das Passwort, bekannt zu geben.

Pharming

Pharming (Domain Spoofing) ist ein zusammengesetztes Kunstwort aus „Password" und „Farming". Wenn der Bankkunde auf seinem PC eine Onlineüberweisung durchführen möchte, wird er automatisch auf die Internetseiten der Betrügerinnen/Betrüger umgeleitet. Die Betrügerinnen/Betrüger erhalten damit die Passwörter bzw. die Geheimzahlen für das Konto der Bankkunden.

1.2.7 Handyviren

Mittlerweile sind auch Smartphones von Virenbefall betroffen. Zahlreiche Computerschädlinge können beträchtliche Schäden, z. B. Zerstörung des Betriebssystems, Ausspionierung von persönlichen Daten, auf Smartphones und Tablets anrichten.

Von Schadsoftware können alle gängigen Smartphone-Betriebssysteme z. B. Apple iOS, Android oder Windows Phone betroffen sein.

Bekannte Viren sind:	
GingerMaster	Private Daten werden ausspioniert und Popups bei der Browserverwendung geöffnet.
mTAN-Trojaner	Nachrichten von Banken werden analysiert und eine Kurznachricht generiert. Darin wird die Userin/der User aufgefordert seinen Benutzernamen und sein Passwort zur Bestätigung einzugeben. Danach werden alle Daten an ein anderes Handy weitergeleitet. Das Bankkonto kann somit geplündert werden.
Battery Doctor	Liest Geräte- und Handynummern sowie E-Mails aus.

So schützen Sie Ihr Smartphone

- Klicken Sie nie auf Werbebanner in kostenlosen Apps: sie werden schnell zur Abofalle.
- Verweigern Sie Apps den Zugriff auf Ortungsdienste und Internetzugang, außer es handelt sich um Navigationsdienste.
- Schalten Sie Ortungsdienste und Bluetooth aus, wenn sie nicht in Gebrauch sind.
- Öffnen Sie keine MMS-Nachrichte von fremden Nummern.
- Nutzen Sie keine unbekannten und ungesicherten WLAN-Netze.
- Speichern Sie niemals Zugangsdaten z. B. zum Onlinebanking auf Ihrem Telefon.

1.2.8 Bots

Hacker nutzen für ihre illegalen Machenschaften Bots (ferngesteuerte Rechner), um anonym zu bleiben. Durch die Einschleusung von Schadprogrammen können Computer ferngesteuert werden. Diese „Zombie-Rechner" werden von Cyberkriminellen auch zu großen Netzwerken zusammengeschlossen – sogenannten **BotNets.** Täglich sind durchschnittlich fast 19 000 Rechner in BotNets in Europa aktiv. BotNets sind oftmals die Ursache vielfältiger Angriffe, z. B. für den Versand von Spam-Mails in großer Zahl. Betroffen sind fast ausschließlich Computer mit dem Betriebssystem WINDOWS.