EICKELSCHULTE®
IT-Betreuung für den Mittelstand

ANLEITUNG ZUM SCHUTZ VOR VERSEUCHTEN E-MAILS

Eine aktuelle und wichtige Information für EICKELSCHULTE-Kunden und deren Mitarbeiter.

Zeitaufwand für dieses Dokument ca. 7 gut investierte Minuten

Ca. 4 Seiten Erklärungen und danach Praxisbeispiele

Sie dürfen auf Grund der Dringlichkeit diese Anleitung an Freunde und Bekannte weitergeben, die nicht Kunde bei EICKELSCHULTE sind.

Schutz vor verseuchten E-Mails

Privat wie geschäftlich werden immer mehr Schriftwechsel, Einkäufe und andere Vorgänge elektronisch erledigt. Dadurch steigt die Gefahr, unerwünschte und/oder schädliche Mails zu erhalten, erheblich. Die negativen Folgen für Sie bzw. Ihr Unternehmen reichen von Belästigung über Erpressung bis zum kompletten Ausfall ganzer IT-Systeme!

Die wirtschaftlichen Folgen dieser verseuchten Spam-Mails einzudämmen und Ihnen Tipps an die Hand zu geben, wie Sie sich richtig verhalten, ist Sinn und Zweck dieser Ausarbeitung. Der Einfachheit halber verwenden wir nur die Bezeichnungen Spam (Oberbegriff) bzw. Malware.

Warum erhalte ich Spam?

Es gibt eine Vielzahl von Programmen, die das Internet gezielt nach E-Mailadressen durchsuchen: auf Webseiten, sozialen Plattformen, in Foren usw. Durch unachtsames Handeln im Internet oder durch Programme/Viren/Trojaner können ganze Adressbücher ausgelesen werden. Beim Surfen im Internet hinterlassen Sie häufig Ihre E-Mailadresse wie z.B. bei Spielen, in Shops, bei Portalen wie z.B. Facebook oder Xing usw.

Oder Sie stimmen AGBs zu, in denen Sie Ihr Einverständnis geben, Werbung zu erhalten und dass Ihre Daten weitergeben werden dürfen. Dadurch landen sie auf unzähligen käuflich zu erwerbenden Adresslisten.

Wie erkenne ich denn Spam-Mails und wie verhalte ich mich?

In der Vergangenheit konnte Spam relativ einfach erkannt werden:
Seltsam-kryptische Absender, ein typischer Betreff (Werbung, Gewinnspiel …), schlechte Grammatik, falscher Satzbau und falsch dargestellte Umlaute waren meist ein eindeutiges Zeichen, dass diese E-Mail Spam war.

Vieles lässt sich auch heute noch mit dem **gesunden Menschenverstand** als Spam identifizieren: Eine ausländische Dame, die Sie auf Facebook gesehen hat, und nun unbedingt Ihre Freundin sein will, ist sehr wahrscheinlich Spam. Und niemand im Internet wird Ihnen einen 500 Euro-Gutschein schenken! Sie können legal kein Geld verdienen, indem Sie als Mittelsmann Ihr Konto zur Transaktion für eine chinesische Firma zur Verfügung stellen … usw.

Andere Mails hingegen **sehen täuschend echt aus:**
Sie werden durch **erfundene** Rechnungen, Inkassoforderungen, Bank- oder anderen Internet-Dienstleistern (Facebook, Ebay, Amazon, PayPal, usw.) dazu aufgefordert, möglichst schnell zu handeln, um angeblichen Schaden zu vermeiden.
Ebenso tückisch: **imitierte E-Mails** von bekannten und häufig genutzten Diensten, die explizit an Sie gesendet werden (z.B. Amazon-Rechnungen zur Weihnachtszeit).
Derzeit am gefährlichsten sind jedoch: persönliche E-Mail Bewerbungen, die sich auf aktuelle Stellenanzeigen aus Ihrem Hause beziehen. Fehlerfrei formuliert und mit Echtdaten gespickt, ist es extrem schwer, diese als gefährliche, weil virusverseuchte Mail zu erkennen!

Der am stärksten gefährdete Personenkreis sind Sie, der pflichtbewusste Mitarbeiter! Sie reagieren am ehesten auf Aufgaben und Dringlichkeiten. Die am meisten angesprochenen Bereiche in einem Unternehmen sind **Vertrieb, Personal und die Buchhaltung**. Ebenso allgemeine Kontakt-E-Mailadressen (info@...)

Vorsicht bei ungewollten Newslettern:
Diese bieten häufig einen Link zum Abbestellen an. Hier führt der Link oft auf eine sogenannte Phishingseite, die versucht, Sie zu einer Eingabe von reellen Daten zu bringen. Diese besser im Outlook als Junkmail kennzeichnen.

Malware kann großen Schaden anrichten:
Sie erhalten eine E-Mail, die Sie dazu bringt, auf einen Link zu klicken und dort eine Datei herunterzuladen oder auszuführen. Oder Sie sollen einen Anhang öffnen, der dann Ihrem Rechner, dem ganzen Netzwerk und all Ihren Daten Schaden zufügt. Eine Version geht so weit, Ihre Daten quasi als Geisel zu nehmen und für die Wiederherstellung Geldbeträge zu verlangen. (Locky Virus Anfang 2016).

Seien Sie vorsichtig und prüfen Sie!

- Fordert Sie die E-Mail zu „unverzüglichem“ oder „schnellem“ Handeln auf? Verdächtig …
- **Angeblich** laufen Kennwörter ab oder sind Systemumstellungen nötig.
- Sie haben angeblich verdächtige Konto-Bewegungen, es seien Rechnungen nicht bezahlt, es droht ein Inkasso Verfahren. Oder Sie erhalten **Rechnungen von Diensten, die Sie gar nicht gebucht haben!** Lassen Sie sich nicht verunsichern!
- Ist die Absenderadresse oder Antwortadresse wirklich die Adresse des Dienstes? Hier werden oft **ähnliche Domänennamen** verwendet; oder absolut unterschiedliche, die aber beim ersten Lesen keinen Verdacht erwecken.
- Ist am Inhalt der E-Mail Verdächtiges zu erkennen? Weicht der Aufbau von originalen E-Mails des Dienstleisters ab? Wenn Sie sonst keine E-Mail von diesem Dienstleister erhalten, oder **nicht Kunde** sind, erübrigt sich dies natürlich!
- Besonders **gefährdende** Datei-Endungen sind: **.exe, .com, .vbs, .bat, .sys, .reg** Diese Dateien sind nicht im normalen E-Mail-Verkehr gebräuchlich.
- Ebenso gefährlich: **doppelte Dateiendungen**, um eine andere Datei vorzutäuschen: Datei.**zip.js** oder Bild.**pdf.exe**
- Verweisen Links in der E-Mail auf falsche Adressen?
- Die E-Mail fordert Sie auf, Benutzernamen und Passwörter, TAN-Listen oder sonstige Eingaben zu machen, um diese zu missbrauchen.
- Wenn Ihr **Virenscanner anschlägt, löschen** Sie die E-Mail, und versuchen nicht, diese auf anderen Weg zu nutzen.
- Auch eine namentliche Ansprache, mit Ihren Daten und bezugnehmend auf aktuelle Umstände (z.B. ausgeschriebene Bewerbung, Gesuche auf Xing oder FaceBook) **bedeutet nicht**, dass die E-Mail keine Malware ist!
- Wenn Sie doch auf ein Word-Dokument geklickt haben und Word möchte **„Makros aktivieren“: ablehnen oder abbrechen! Gleiches gilt für Excel und pdf-Dateien !**

Klicken Sie *nicht* auf Links in solchen E-Mails! Laden sie *keine unbekannten* Dateien herunter und prüfen Sie genau, welche Dokumente Sie öffnen.

Wie schütze ich mich vor Spam, Malware und Co?

Grundsatz: Versuchen Sie, mit Ihrer E-Mailadresse **sorgfältig** umzugehen! Geben Sie diese nicht an jeden beliebigen weiter.

- Tragen Sie sich **nur** in Newsletter und Mailinglisten ein, die Sie wirklich erhalten möchten. Prüfen Sie die Angaben, ob und wie Ihre E-Mail weitergegeben wird.
- **Löschen Sie erkennbare Spam-Mails direkt, antworten Sie nicht** und **reagieren Sie auf keinen Fall** auf dessen Inhalt! **Klicken Sie nicht auf Links, und öffnen Sie keine Anhänge.**
- Seien Sie besonders vorsichtig bei Sammel-E-Mailkonten wie „info@“ oder „bewerbung@“, diese sind sehr häufig Ziel von Spam-E-Mails.
- Lassen Sie sich die E-Mails in der Vorschau als „Nur-Text“ anzeigen. Bilder und Dateien werden als Anhang angezeigt.
- Lassen Sie im Windows Explorer **die „echten“ Dateiendungen anzeigen**:
  bei Windows 10 unter dem Reiter Ansicht den **Haken bei „Dateinamenerweiterungen“** setzen; bei Windows 7 in den Ordneroptionen den Haken bei **„Erweiterungen bei bekannten Dateitypen ausblenden“ entfernen**
- Öffnen Sie nur E-Mails von Absendern, **die Sie kennen** und von denen Sie sicher sein können, dass die E-Mail auch vom erwarteten Absender kommt. Ist Ihnen der Absender unbekannt und die E-Mail verdächtig, **fragen Sie beim Absender telefonisch** nach, was er Ihnen schicken wollte.
- Gehen Sie **manuell auf die offizielle Webseite** Ihres Dienstleisters (Amazon, PayPal, Telekom …) und prüfen dort nach, ob verdächtige Kontoaktivitäten vorliegen.
- Nutzen Sie zum kontrollierten Austausch von Daten keine E-Mail, sondern einen **sicheren verschlüsselten Datenraum**, in dem Sie Daten für andere ablegen können. Dieser Datenraum wird bei Bedarf vom Arbeitgeber zur Verfügung gestellt!
- Sorgen Sie dafür, dass Ihre Daten immer in ein Backup-Verfahren integriert sind, und regelmäßig ein **Backup** erstellt wird, welches anschließend vom Netzwerk oder dem Rechner getrennt wird. (Andernfalls können auch die Backups zerstört werden!)
- **Sorgen Sie dafür, dass Ihr Rechner immer auf dem aktuellen Stand ist, spielen Sie regelmäßig Updates ein, sorgen Sie dafür, dass Ihre Virensoftware aktuell ist.**

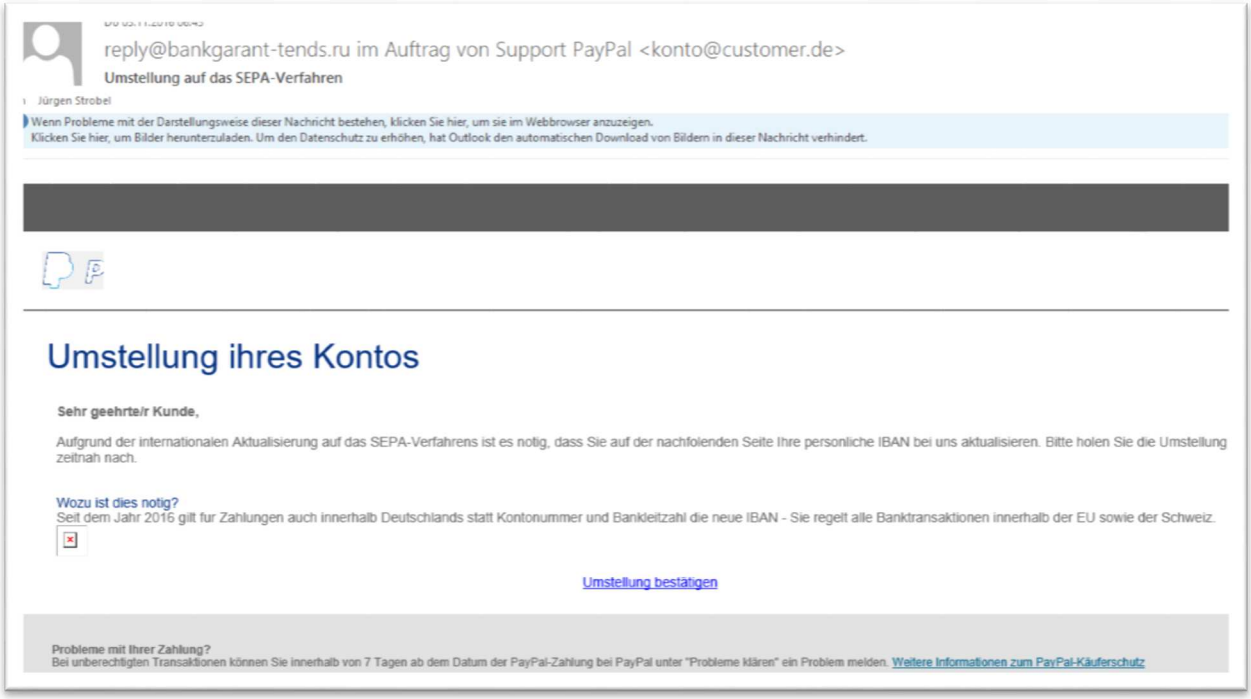
Wenn Sie diese Tipps beachten, reduzieren sich unerwünschte Mails und das Risiko, dass Ihre IT Schaden erleidet, deutlich.

Trotzdem werden Sie noch etwas Spam erhalten - denn auch der beste Virenscanner, der beste Spamfilter kann keine 100%ige Sicherheit geben. Und: Hersteller von Virenscannern können immer erst **nach** dem Auftreten von neuer Schadsoftware **darauf reagieren**. Was also gestern noch aktuell und geschützt war, kann heute schon unsicher sein.

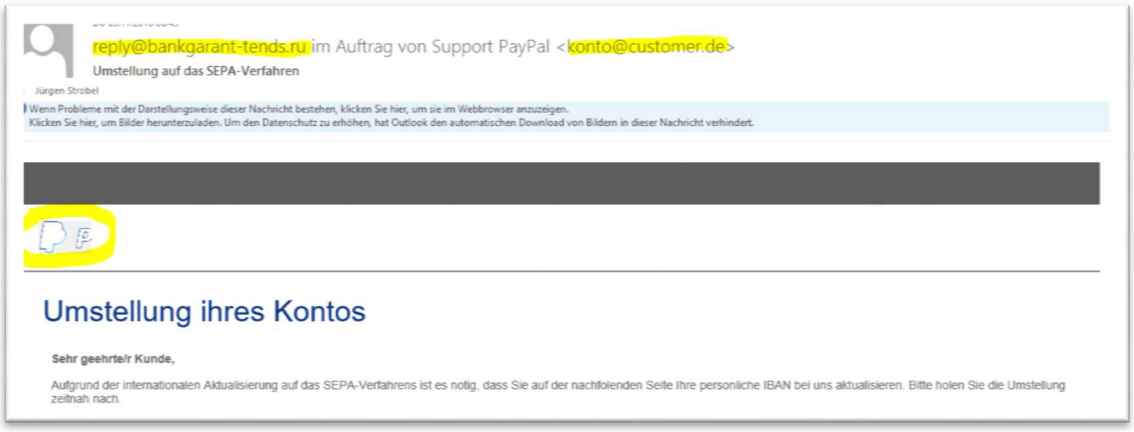
Manchmal schießen Spam-Filter aber auch über das Ziel hinaus und sortieren eigentlich gewünschten Inhalt aus. Das System versucht hier nur, durch viele Faktoren eine Entscheidung zu treffen. Ein regelmäßiger Kontroll-Blick in den Spam-Ordner schafft Klarheit und lässt unbekannte Absender nach oben beschriebener Prüfung ggf in den „Erwünscht-Ordner“ verschieben.

Beispiele - hätten Sie sie als Spam erkannt?

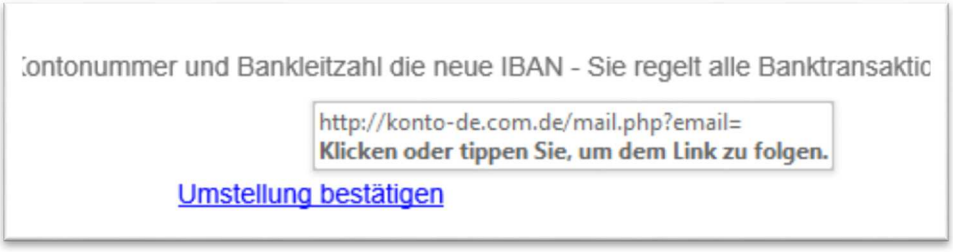
Eine Spam-Mail über eine **PayPal Umstellung,** in der behauptet wird, das Konto solle auf ein SEPA-Verfahren umgestellt werden.



Hier fallen mehrere Dinge bei genauer Betrachtung auf:

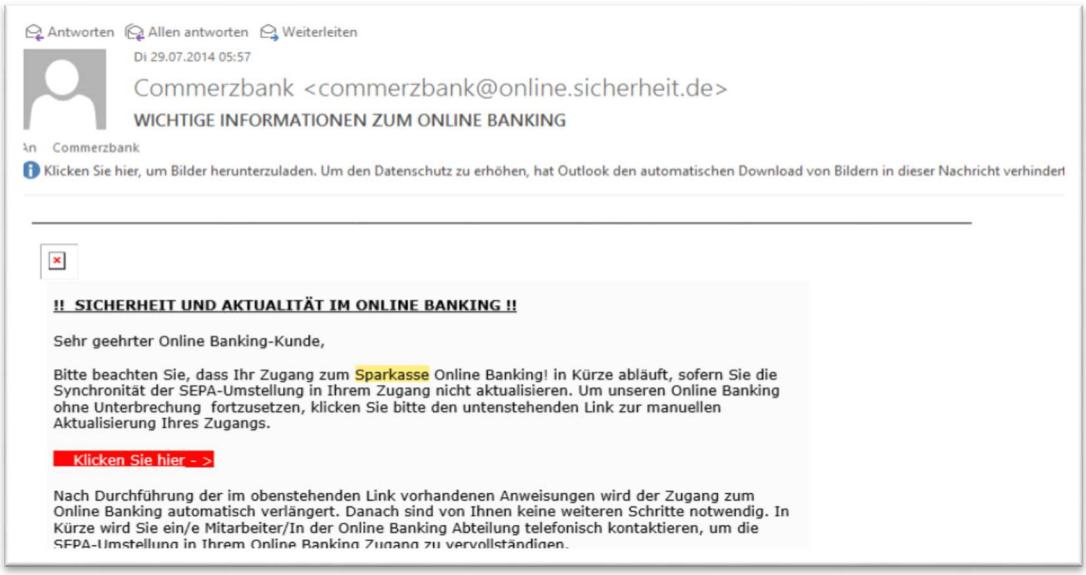


1. Das PayPal Logo ist sichtlich nicht in Ordnung.
2. Der Email-Absender ist reply@bankgarant-tends.ru -> ru=Russland!
3. Das angegebene Konto ist konto@customer.de Wird diese Adresse bei Google (nicht in der Adressleiste des Browsers!) eingegeben, kommen viele Treffer, die Warnungen enthalten.
4. Wird mit dem Maus Cursor über den Link **gestriffen** (**nicht klicken!),** wird die Zieladresse angezeigt: konto-de.com. **Dies ist keine Adresse, die auf PayPal schließen lässt!**



Weitere Beispiele

Commerzbank E-Mail bzgl. Aktualisierung von Kontodaten wegen Ablauf eines **Sparkassen** Online Zugangs?! ☺



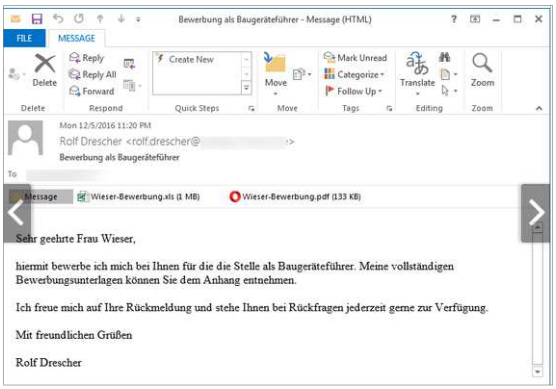
Täuschend echte DHL Nachricht:

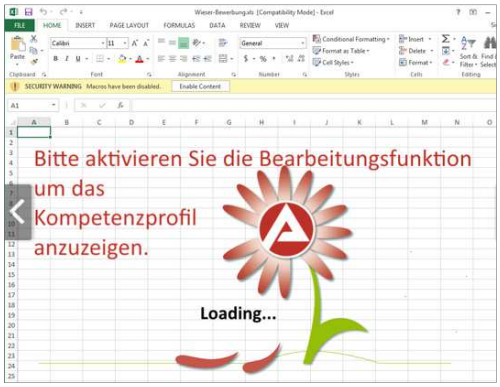
Rechnungen von Vodafon, obwohl wir gar nicht bei Vodafon Kunde sind. ☺

Und ein weiteres, besonders folgenschweres Beispiel:

Eine Firma schaltet ein **Stellengesuch** bei einschlägigen Portalen (z.B. Monster.de). Die Portale sind untereinander meist mit anderen Portalen verknüpft. D.h. Ihr Stellengesuch wird auch auf anderen Portalen sichtbar.

Zu gleichen Zeit kommt diese Email an Ihre Personalabteilung:





Der arglose Mitarbeiter öffnet den Anhang, für das Ausführen eines Makros erscheint die Warnung. diese wird verhängnisvoller Weise zugelassen und das Ergebnis kommt direkt. Der Rechner geht aus, startet neu und dies begrüßt den Mitarbeiter:

Ihr Rechner und evtl. Daten im Netzwerk, auf die der Benutzer Zugriff hat, wurden verschlüsselt und sind somit wertlos! Sie werden aufgefordert, Lösegeld zu bezahlen. Das sollten Sie natürlich nicht tun.

Fazit:

Mit diesem Wissen sollten Sie gerüstet sein, um verseuchte E-Mails zu erkennen und entsprechend zu handeln. Auch sind Sie mit diesem Wissen vielen Anwendern voraus. Teilen Sie Ihr Wissen ☺

Allerdings: Diese Ausarbeitung erhebt keinen Anspruch auf Vollständigkeit. Eine Haftung kann deshalb nicht übernommen werden.

Für Rückfragen oder konkreten Fällen steht Ihnen das Team der EICKELSCHULTE gern zur Verfügung.

Tel.: 08151 77040
www.eickelschulte.de
info@eickelschulte.de

Bei aller Achtsamkeit ist weiterhin die wichtigste Vorsichtsmaßnahme: Stellen Sie sicher, dass Sie immer aktuelle Backups von Ihren Daten zur Verfügung haben.