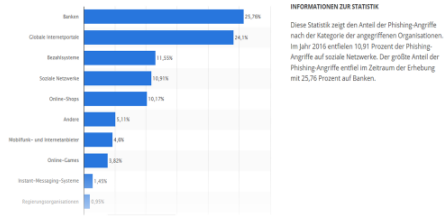
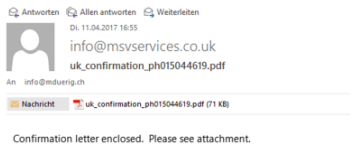
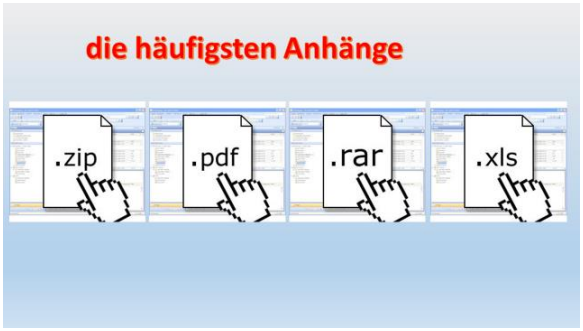
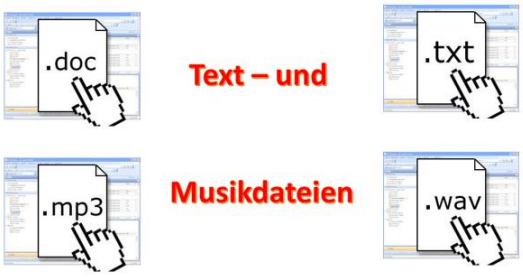
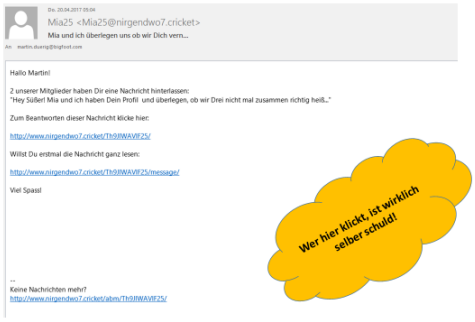
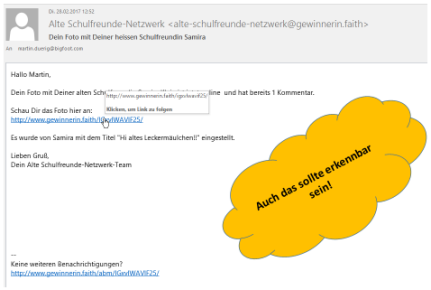
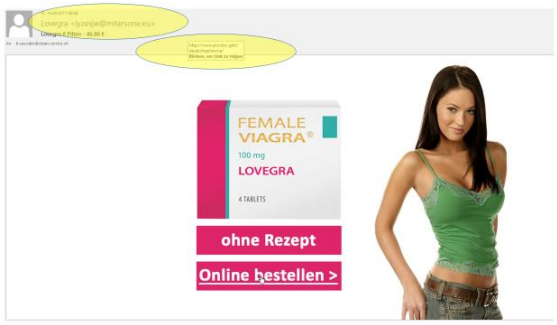
Phishing Mails

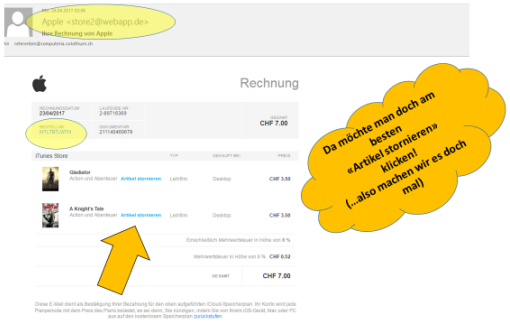
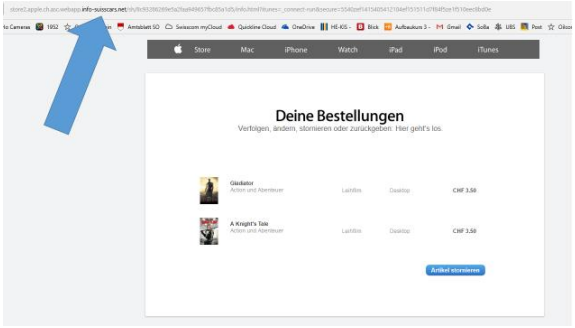
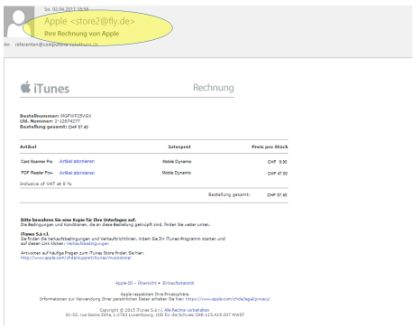
Computeria 27.April 2017
Martin Dürig

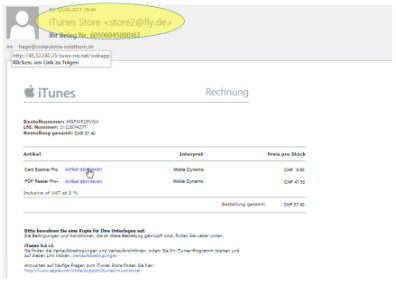
	Phishing Mails Martin Dürig
	Viele haben vor noch nicht allzu langer Zeit ein solches oder ähnliches Mail von der swisscom erhalten und gestaunt. Hier handelt es sich um ein gut gemachtes Phishing Mail
Was ist Phishing? Das Wort Phishing setzt sich aus den englischen Wörtern «Password», «Harvesting» und «Fishing» zusammen.	Nach der Definition geht es darum, dem Anwender Passwörter zu entlocken.
	Darum erste Regel: Gib nie deinen Benutzernamen und dein Passwort weiter, vor allem nicht per Mail.

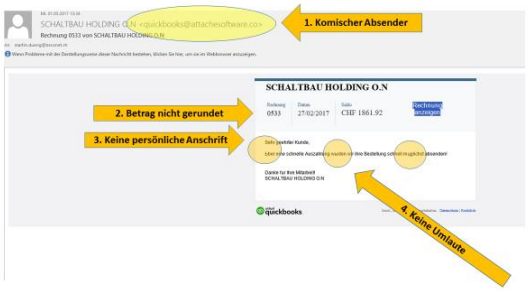
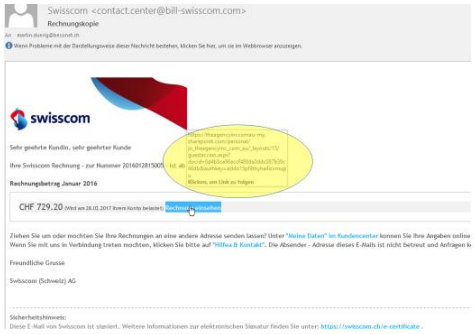
Nicht nur die Masse an Spam-Mails nahm im vergangenen Jahr erstmals nach 2010 wieder deutlich zu. Laut dem jährlichen Cybersecurity Report von Cisco, ein US-Unternehmen für Internetlösungen, wurden 2010 pro Sekunde 5000 verschickte Spams registriert. Diese Zahl sank in den folgenden Jahren auf 1500 bis 2000 verschickten Spams, während **im Jahr 2016 wieder 5000 Spam-Mails pro Sekunde notiert wurden.**	Es kursieren Unmengen von schädlichen Mails im Netz herum. 5000 pro sec 300'000 pro min 18'000'000 pro h 432'000'000 pro Tag 158'775'000'000 pro Jahr
Anteil der Phishing-Angriffe nach Kategorie der angegriffenen Organisationen im Jahr 2016  INFORMATIONEN ZUR STATISTIK Diese Statistik zeigt den Anteil der Phishing-Angriffe nach der Kategorie der angegriffenen Organisationen. Im Jahr 2016 entfielen 10,91 Prozent der Phishing-Angriffe auf soziale Netzwerke. Der größte Anteil der Phishing-Angriffe entfiel im Zeitraum der Erhebung mit 25,76 Prozent auf Banken.	Natürlich haben es die Betrüger in erster Linie auf Geldinstitute abgesehen
Eine Schadstoff-Software oder eine Spionage-Software kommt **NIE von selbst** auf meinen Computer!  Ich selber bin verantwortlich und habe sie mit Doppelklick installiert…	Schuld an eingeschleppten Spionage-Software hat immer der Benutzer oder die Benutzerin. Die schädlichen Programme verstecken sich aber sehr gut, meist hinter andern Dateien oder hinter anklickbaren Links
 Antworten Allen antworten Weiterleiten Di. 11.04.2017 16:55 info@msvservices.co.uk uk_confirmation_ph015044619.pdf An info@mduerig.ch Nachricht uk_confirmation_ph015044619.pdf (71 KB) Confirmation letter enclosed. Please see attachment.	Einige Mails sehen schon auf den ersten Blick verdächtig aus. Hier ein PDF-Anhang, der geöffnet werden soll.

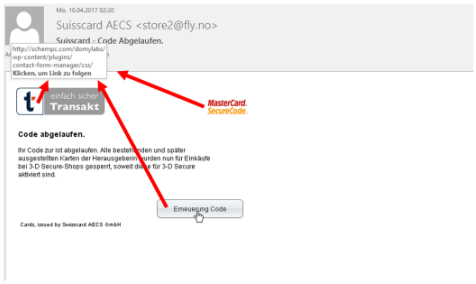
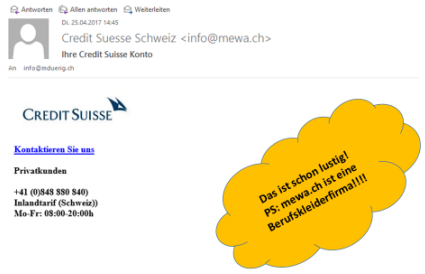
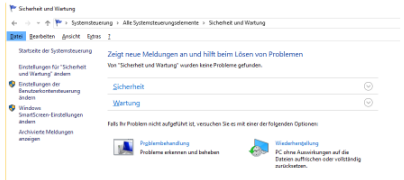
	Die häufigsten Schadstoff-Programme verstecken sich hinter diesen 4 Dateien: .zip komprimierte Datei .pdf ein PDF-Dokument .rar komprimierte Datei .xls Excel-Datei
	Aber auch in Dateien, die mit Doppelklick gestartet werden: .bat Stabelbefehlsdatei .com Befehlsdatei .exe ausführbare Datei .reg verändert die Registry .vbs Visual-Basic Scriptdatei (kein Zusammenhang mit Bundesrat Parmelin!)
	Aber auch die können Gefährliches enthalten: .doc Word-Datei .txt Text-Datei .mp3 Musik-Datei .wav Musik-Datei
	Und zu guter letzt: .asf Video-Datei .avi Video-Datei .mov Video-Datei .mpg Video-Datei .gif Grafik-Datei .jpg Bild-, Foto-Datei .html Internetseiten-Datei

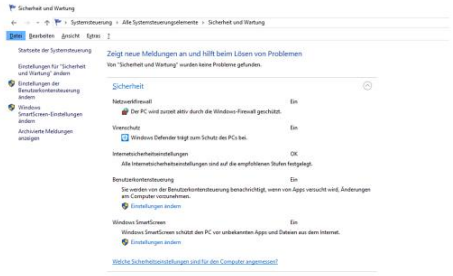
Beispiele **von Phishing-Mails** **eines Anwesenden hier im Saal** **(Name bleibt geheim)**	Alle gezeigten Beispiele sind authentisch
	Solche Mails bekommen wir alle immer wieder. Sie sind so auffällig und einfach gestrickt, dass sie sofort erkannt werden.
	Das tönt schon plausibler. Zu beachten: Genau schauen, wohin der Link führt. Die Internetadresse ist ersichtlich
	Viagra für Frauen????? Absenderadresse beachten! Das ist sehr komisch

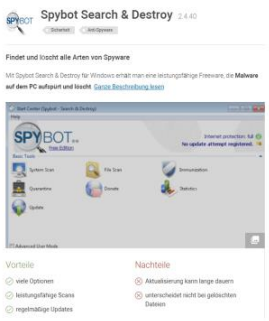
	Die Idee von Geld erschwindeln ist nicht neu und funktioniert nach wie vor.
	Ein schon besser gemachtes Mail! Die Rechnung sieht wie echt aus, ich bekomme ja von Apple fast gleiche, wenn ich eine App kaufe. Hier aber habe ich weder das eine noch das andere Spiel gekauft. "Stornieren" wäre eine Versuchung, aber das steckt ja das Problem drin!
	Ich habe es trotzdem gemacht und hier bitte mal die Adresse beachten! Das kann nicht gut gehen – also nicht weiter anklicken und löschen. Sieht aber sehr echt aus!
	Auch noch eine Rechnung von Apple, diesmal von iTunes. Die Artikel habe ich nicht gekauft und Apple verschickt sicher keine Rechnungen von fly.de!

	Auch hier könnte ich wieder stornieren, lande mit dem Link aber bei **46.32.240.35/swiss-rxr.net**
	
	VERDÄCHTIG!
	46.32.240.35 Ist eine Domain namens
	`HEART-INTERNET`
	`In Leeds, GB`

	Die wichtigsten Merkmale einer Phishing-Mail: 1. Absender verdächtig 2. Bei Geldbeträgen nicht gerundet 3. Anrede mit "Kunde / Kundin" 4. Im Text keine Umlaute, oft Schreibfehler
	Zurück zum Einstiegsbeispiel: "Rechnung einsehen" führt zu einem englischen, undefinierbaren Link
	Auch dieses Mail sieht täuschend echt aus. Die Absenderadresse kennen wir doch… Diesmal aber fly.no Das Problem …

	…. alle 3 anklickbaren Links für auf die gleiche Seite!
Merkmale der Phishing-Mail: • Der Kunde wird **nicht persönlich angesprochen**, sondern nur mit «Sehr geehrte Kundin, sehr geehrter Kunde» • Rechnungsbeträge werden **auf den Rappen genau** ausgestellt (z. B. 691.81 oder 929.33 Franken). Die Swisscom rundet diese immer auf. • **Umlaute wie ä, ö oder ü fehlen**. Generell sollte man bei **Mails mit Rechtschreibfehlern** skeptisch sein, da standardisierte Benachrichtigungen an die Kunden mehrmals geprüft worden sind. • Scheint die **Absender-Adresse** für das Unternehmen **wenig plausibel** oder ist diese sehr lang, handelt es sich meistens um Phishing. Am Absender «sme.contactcenter@bill.swisscom.com» kann man relativ einfach erkennen, dass die Firma nicht über eine solche Mail-Adresse verfügt.	
	… und hier noch ein Beispiel einer gehackten Mailadresse: info@mewa.ch existiert wirklich! Ist eine Berufskleiderfabrik! Was heisst wohl "Credit Suesse Schweiz" ?
Ist mein Computer sicher? Wartungscenter in Windows kontrollieren: Starten des Wartungscenters durch Eingabe von ***wscui.cpl*** *in das Eingabefeld des Windows-Startmenüs* oder Menü «Windows-System – Systemsteuerung – Sicherheit und Wartung» 	Die wichtige Frage: Ist mein Computer sicher oder schon gehackt worden?

	Im Wartungscenter die Sicherheit kontrollieren und allenfalls anpassen gemäss Beispiel.
	... und sollte ich doch mal falsch geklickt haben Ruhig Blut bewahren
	Leider fehlt diese Taste auf den meisten Compis
	Dieses Programm sollte installiert werden und ab und zu auch verwendet werden!

	Im Explorer suchen nach "Spybot Search and Destroy" und installieren
	Voilà! Ziel erreicht!