Richtlinien & Empfehlungen

für

Nutzer der geschlossenen Facebookgruppe

Victorface

Ev.-luth. Kirchengemeinde Victorbur

22. Juli 2013
Version 1.1

Inhaltsverzeichnis **Seite**

0. Allgemeines

0.1 Dokumentation der Fortschreibung

Version	Datum	Betreff Kapitel/Inhalt	Seiten
1.0	10.07.2013	Entwurfsversion zur Sitzung des Kirchenvorstands am 16. Juli 2013	1-17
1.1	22.07.2013	Version zur Versendung der Richtlinien an den Kirchenvorstand der Kirchengemeinde Victorbur zum Zweck der Genehmigung **du**rch den Kirchenvorstand	1-19

0.2. Quellennachweis

Facebook-Datenschutzrichtlinien vom 15. Dezember 2010 um 17:04
https://de-de.facebook.com/note.php?note_id=10150367530590301&id=69178204322

facebook - Das ultimative Handbuch - Ein Sonderheft von CHIP - Ausgabe 2012

Meine Kinder in sozialen Netzwerken – BVDW – Social Media

Orientierungshilfe „Soziale Netzwerke“ – Konferenz der Datenschutzbeauftragten des Bundes und der Länder – 14.03.2013

„Mediatisierte Welten" - Deutsche Forschungsgesellschaft (DFG)

0.3. Zweck des Dokuments

Mit Beschluss des Kirchenvorstands vom 15. Mai 2013[1] wird in der ev.-luth. Kirchengemeinde Victorbur eine zunächst geschlossene Facebook-Gruppe eingerichtet. Sie soll im Gemeindeleben als ergänzendes Kommunikationsmittel, insbesondere für Kinder, Jugendliche und junge Erwachsene dienen.

Der weltweite Anstieg der Facebook-Nutzer auf fast 1 Milliarde hat mit der Sehnsucht eines Heranwachsenden zu tun, dass es da jemanden geben möge, der in ihm den Menschen ansieht, der er ist. Trotzdem fällt es schwer, die ökonomischen Ziele und das Gefahrenpotential von Facebook zu akzeptieren

Was ist zu tun? Auf Facebook verzichten? Für unsere Gemeinde ist dies keine ernsthafte Alternative, da wir junge Leute nur so erreichen und wir auf die angebotenen Veranstaltungen, insbesondere auf das Angebot für junge Leute in unserer Gemeinde nur auf diese Weise hinreichend aufmerksam machen können.

Die einzige Möglichkeit hier einen sicheren Weg zu gehen, ist dieses Dokument, das das Gefahrenpotential (Kapitel 1) aufzeigt und zur Gefahrenabwehr Empfehlungen und Richtlinien als Voraussetzungen zur Teilnahme (Kapitel 2) der Gruppenmitglieder nennt.

Die Freigabe der geschlossenen Facebook-Gruppe **victorface** einschließlich der Facebook-Website erfolgt erst nach Genehmigung dieses Dokuments **Du**rch den Kirchenvorstand.

Der Kirchenvorstand

[1] [1] Protokoll über die Sitzung des KV vom 15.05.2013. TOP 4: Gemeindeleben d)aus dem Ausschuss für Öffentlichkeitsarbeit (Hiller/Schmidt; Beschlussvorlage Facebook)

1. Einleitung

1.1 Soziale Netzwerke

Der Hauptgrund, warum so viele Jugendliche soziale Netzwerke, insbesondere Facebook nutzen ist die Tatsache, dass Freunde und Bekannte auch im Netz drin sind.

„Ich wurde jeden Tag darauf angesprochen, mich jetzt doch endlich mal bei Facebook anzumelden. Freunde forderten mich sogar per SMS dazu auf."

Soziale Netzwerke sind lokal, denn **Du** bist hauptsächlich mit den Freunden zusammen, die man auch sonst in der Schule, im beruflichen Umfeld, im Jugendkreis oder im Verein trifft. Aber auch der virtuelle Raum Facebook ist ein Raum, in dem man zusammen sein kann, auch wenn man räumlich getrennt voneinander ist.

Ein soziales Netzwerk hat eine kommunikative Funktion; mit den Freunden Kontakt zu haben, sich zu verabreden, auf Ereignisse hinzuweisen, sich selbst den Freunden zu präsentieren. Zur Selbstpräsentation gehört die Einstellung attraktiver Fotos um zu zeigen, wie man gerne sein möchte. Wichtig ist in einem Alter, in dem man seine Identität herausbildet, die Funktion der Orientierung. Da schaut man andere Profile in Facebook an, schaut nach, wie sich andere darstellen. **Du** postest Fotos von Dir ins Netz und wartest, welche Resonanz kommt. Das Netzwerk ist also ein Ort der aktiven Auseinandersetzung mit der eigenen Persönlichkeit.

Welcher Trend ist bei den sozialen Netzwerken zu beobachten?

- Facebook wird zunehmend mehr **aktiv** genutzt. Das heißt: **Du** greifst zunehmend selber aktiv mit Beiträgen ein.

- Die Nutzung resultiert vor allem darin, abzustimmen über eine Angelegenheit und das Niederschreiben persönlicher Ansichten in ein Formular.

- Eine stärker werdende Konzentration auf den Computer und mobile Geräte als Universalmedium bei gleichzeitigem Sehen und Hören von Fernseh- bzw. MusiksenDungen im Radio.

- Facebook verdrängt den Stellenwert des Maildienstes. Man hat zwar eine Mailadresse aber nutzt sie nicht für die Kommunikation. Das heißt, **Du** und Deine Freunde sind über den klassischen Maildienst **nicht** erreichbar.
  Bei mobilen Geräten ist es genau umgekehrt, sie dienen aufgrund ihrer Multifunktionalität als Grundlage zur Nutzung sozialer Netze.
- Wir leben in einer zunehmend exhibitionistischen Gesellschaft in der uns von den Medien und der Werbung vorgelebt wird, dass die öffentliche Präsentation des IndiviDuum sehr wichtig ist. Warum solltest **Du** Dich davon ausnehmen?

1.2 Gefahrenpotential in sozialen Netzwerke

1.2.1 Facebook vergisst nichts

Soziale Netzwerke sind Lebensräume wie andere auch. In dem Bewusstsein der Jugendlichen unterscheiden sich diese Lebensräume in ihren Gesetzmäßigkeiten nicht von realen Räumen. Im realen Leben spielt Zeit eine wichtige Rolle. Im virtuellen Raum ist die Zeit nicht existent. Was im Netz präsentiert wird, bleibt **ewig öffentlich existent** und wirkt auch dann noch wenn **Du** in einem Alter bist, indem **Du** Dich eventuell für eine solche Präsentation schämen würdest.
Weiterhin besteht die Gefahr, dass **Du** Dich selbst durchsichtig machst und Dich somit der

kommerziellen Ausnutzung durch Deine veröffentlichten, persönlichen Daten auslieferst. Man liefert alle Daten über sich selbst. Der Betreiber des sozialen Netzwerks schöpft diese Daten ab, bereitet sie auf für das Marketing, verkauft sie und macht damit riesige Gewinne.

1.2.2 Cyber-Mobbing

Cybermobbing gehört zum Alltag vieler Kinder und Jugendlicher in Deutschland. "Mädchen werden gerne in die Schmuddelecke gestellt, als Schlampe diffamiert", Jungen werden oft als "Homosau" fertiggemacht. Man versucht, ihnen Pornos mit Männern anzuhängen. Das Cybermobbing kann viel schlimmer und dramatischer sein, als Mobbing auf dem Schulhof im kleinen Kreis. Früher fühlten sich die Opfer zuhause sicher. Aber heute gibt es keinen Schutzraum mehr. Die Cybermobber kommen ins Kinderzimmer." Der Terror läuft oft über einen langen Zeitraum. Das Mobben via Foto und Video kommt zwar vergleichsweise selten vor, belastet die Jugendlichen aber besonders stark. Auch der Verrat von Geheimnissen kränkt und verletzt. Die jugendlichen Opfer allein können es nicht schaffen.

1.2.3 Cyber-Kriminalität

Soziale Netzwerke sind für Sexualstraftäter und Menschen mit kriminellen Absichten eine einladende Plattform und Heranwachsenden oft nicht bewusst. Kriminelle sind mit zunehmendem Erfolg dabei Konten von Internet-Usern abzuräumen. Es gibt kaum noch ein bekanntes soziales Netzwerk wo nicht bereits zahlreiche Mitglieder zum Teil erhebliche Summen mit immer neuen Methoden verloren haben. Facebook mit seinen fast 1 Milliarde Nutzern ist ein besonders lukratives Betätigungsfeld für Kriminelle, denn viele Facebook-Nutzer hinterlegen neben ihren rein privaten Daten auch ihre Bankverbin**Du**ngen.

Insbesondere stellt hierbei der „Like"- oder „Gefällt mir-Button" eine Gefahr dar. Viele User überlegen nicht lange und klicken auf die Aufforderung. Diese gutmenschliche Reaktion machen Internet-Kriminelle zu ihrem alleinigen Vorteil indem Sie erst einmal Zugangsdaten erbeuten um dann sämtliche versteckten Informationen von betroffenen Nutzern abgreifen und um gleichzeitig auch ihre "Phishing" Bildchen in weitere Freundeskreise unterzubringen, womit sehr schnell gar mehrere Millionen Klicks, aber auch tausende Opfer, zusammenkommen können.

Auch Rechtsextreme nutzen immer mehr soziale Netzwerke, um Parolen zu verbreiten und damit junge Menschen zu ködern Neben sozialen Netzwerken nutzen sie auch QR-Codes[2] oder Apps, um Jugendliche auf ihre Seiten zu locken.

Übrigens: Stalking, d.h. Personen willentlich und wiederholt verfolgen und belästigen, ist nach deutschem Recht ein Straftatbestand, egal ob auf der Straße und per Mausklick auf Facebook.

1.2.4 Infizieren mit Schadsoftware

Soziale Netzwerke werden zunehmend von hochintelligenten Kriminellen zur **Verbreitung von Schadsoftware** genutzt. Neben der Gefahr, auf infizierte Webseiten geleitet zu werden, werden soziale Netzwerke auch verstärkt genutzt, um Passwort-Phishing (Ausspähen von Pass- bzw. Kennwörtern) zu betreiben. Grundsätzlich sollten Nutzer daher wie bei allen Internetanwen**Du**ngen auch in sozialen Netzwerken vorsichtig sein und nicht wahllos auf Links klicken. Schwachstellen in Facebook sind grundsätzlich unabhängig vom verwendeten Webbrowser ausnutzbar.

[2] QR=Quick Read. Mit einer QR-Apps auf dem Smartphone wird der QR-Code gescannt und man gelangt direkt auf die entsprechende Website.

1.2.5 Verletzung des Urheberrechts

Wer Fotos, Filme, Texte oder Musikstücke ohne Erlaubnis mit der Funktion "Hochladen" auf seine Facebook-Seite stellt, verstößt gegen das Urheberrecht – und das kann teuer kommen.
Zum Beispiel das Hochladen von urheberrechtlich geschützter Musik, die gerade angesagt ist, downgeloaded von der Plattform YouTube, auf die eigene Facebook-Seite. Die Rechtslage ist eindeutig: Wer sie hochlädt, verbreitet die urheberrechtlich geschützten Stücke gleichzeitig illegal weiter. Diverse Anwaltskanzleien haben sich inzwischen darauf spezialisiert, die meist jugendlichen Nutzer mit Abmahnungen in horrender Höhe zu überziehen. Unwissenheit schützt, wie so oft, vor Strafe nicht. Und auf der bleiben dann meist Deine Eltern sitzen

Noch ist es schwierig, die Vergehen zu ahnden. Für einige Medienrechtsexperten ist es allerdings nur eine Frage der Zeit, bis dies erleichtert wird. Und da das Internet nichts vergisst, kann man sich vor dieser möglichen Entwicklung gar nicht früh genug schützen.

2. Richtlinien und Empfehlungen

Die nachfolgenden Richtlinien (Policies) sind Verhaltensregeln denen sich ein Mitglied der geschlossenen Facebookgruppe **victorface** unterwirft. Ein Verstoß gegen diese Richtlinien führt zur Abmahnung durch den Gruppenadministrator. Bei einem zweiten Verstoß gegen die Richtlinien wird das Mitglied vom Administrator aus der Gruppe entfernt.
Bei jedem Mitglied, das der geschlossenen Gruppe beitritt, werden Kenntnisse zur Nutzung mit Facebook vorausgesetzt. In Kapitel 3. werden unverbindliche Empfehlungen ausgesprochen, die zur Erhöhung der Sicherheit der einzelnen Mitglieder und der Gruppe dienen.
Darüber hinaus gelten die Facebook-Datenschutzrichtlinien die **Du** als Facebook-Mitglied bei Registrierung akzeptierst und auch einhalten musst.
Weiterhin geben wir Dir Empfehlungen für eine sichere Nutzung der Facebook-Plattform.

2.1 Dein Profil Facebook anlegen / anpassen

Kategorie: Empfehlung

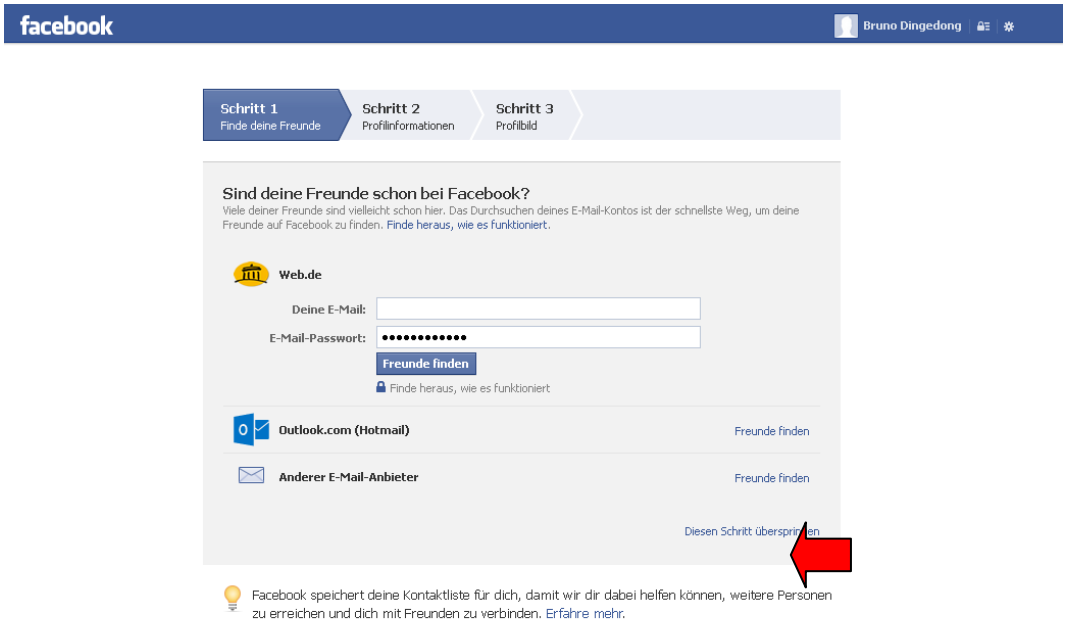
Gefahrenpotential: Kapitel 1.2.1 Facebook vergisst nichts.

Voraussetzung zum Beitritt in die geschlossene Facebookgruppe **victorface** ist Dein eigener Facebook-Acount.
Auf der Facebook-Internetseite https://de-de.facebook.com/ kannst **Du** Dich registrieren und die erforderlichen Daten für eine Mitgliedschaft eingetragen.

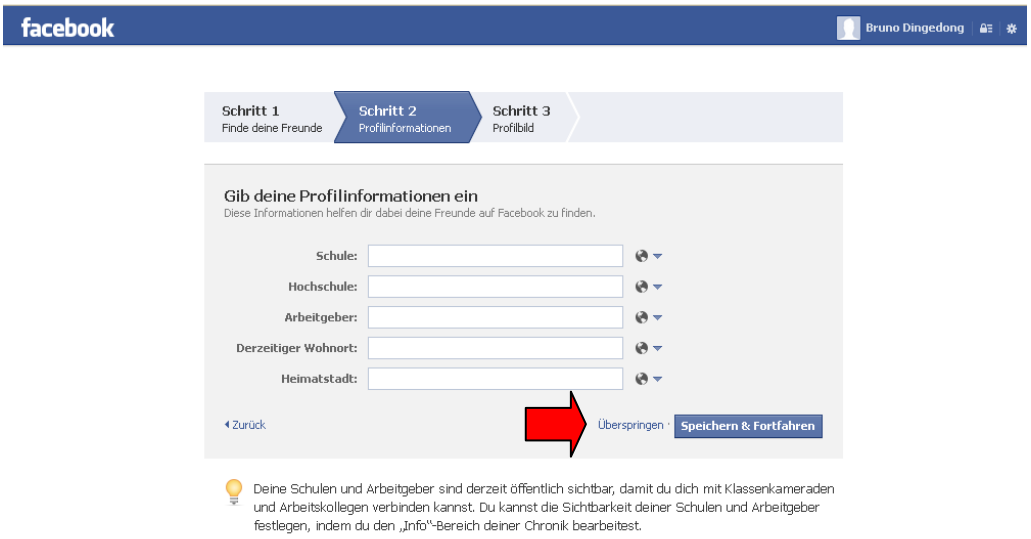
Facebook-Registrierungsbildschirm 1. Seite

Als neuer Nutzer musst **Du** mindestens **13 Jahre** alt sein, sonst wird Dir die Anmeldung verweigert.
Die Funktion ***Freunde finden*** bei Schritt 1 bitte überspringen und später ev. nachholen.
Warum: Facebook **Du**rchsucht auf Wunsch private Email-Postfächer nach Kontakten, die möglicherweise auch bei Facebook registriert sind. Hierfür müssen die entsprechenden Zugangsdaten der Postfächer, also Benutzername und Passwort, eingetragen werden. Facebook verspricht zwar, diese Daten nicht zu speichern, dennoch erlaubt man so einem anderen Unternehmen einen Einblick in die Privatsphäre. Hier musst **Du** als neues Facebook-Mitglied zwischen Nutzen und möglicher Gefahr abwägen.

Je mehr persönliche Daten **Du** eingibt, desto besser wird derjenige gefunden. So kann man beispielsweise nach Freunden und Mitschülern suchen. Zudem werden Dir auch Personen vorgeschlagen, die **Du** möglicherweise kennen könntest. **Du** als Facebook-Frischling solltest Dich sehr zurückhaltend mit der Preisgabe privater Informationen sein. Lerne erst einmal das System Facebook kennen. Erst nach längerer Nutzung erschließen sich Dir die vielfältigen Funktionen.



Privat bleibt privat.
Erinnerst **Du** Dich an die Geschichten von Arbeitgebern, die sich bei Facebook über Angestellte informieren oder Partybilder, die man nüchtern lieber nicht im Internet finden würde. All dies lässt sich leicht über die „Privatsphäre-Einstellungen“ verhindern. So lässt sich festlegen, welche Informationen wem zugänglich gemacht werden. Wir empfehlen Dir, Schritt 2 zu überspringen (roter Pfeil)



Bei Schritt 3 musst **Du** selbst entscheiden, ob **Du** ein Foto von Dir oder einen anonymen Smiley hochladen möchtest. Alles eine Sache des guten Geschmacks.

Mit diesem 3. Schritt bist **Du** nun Mitglied bei Facebook. Und dabei solltest **Du** es auch erst einmal belassen. Und nunmehr kannst Du der geschlossenen Facebookgruppe **victorface** mit ruhigem Gewissen beitreten.

2.2 Abwehr von Cyber-Mobbing

Kategorie: Richtlinie

Gefahrenpotential: Kapitel 1.2.2 Cyber-Mobbing

Soziale Netzwerke leben von persönlichen Kommentaren. Mitunter können aber Deine in die Öffentlichkeit gepostete Kommentare Personen "an den Pranger stellen".

Das Internet vergisst nie. Unerwünschte Einträge lassen sich auch nach Jahren kaum noch löschen, weil die Daten auf ausländischen Servern gespeichert werden, die nicht dem deutschen Recht unterliegen. Prüfe deshalb Deine öffentliche Einträge zeitnah und lösche umgehend Einträge, die Dir selbst oder anderen schaden könnten.

Darum:

Wer als Mitglied der Facebook-Gruppe **victorface** eine Person oder eine Gruppe über die Facebook-Plattform schikaniert, anpöbelt, belästigt, beleidigt, ausgrenzt, mit dem Ziel, diese Person zu demütigen und zu vertreiben, begeht einen Richtlinienverstoß und erhält vom Gruppenadministrator eine Abmahnung, dieses Vorgehen zu unterlassen.

Bei einem weiteren Verstoß wird Dich der Gruppenadministrator aus der Facebook-Gruppe entfernen. Eine erneute Aufnahme in die Gruppe ist dann nicht mehr möglich.

Halte Dich an Folgendes:

- **Du** postest nur Nachrichten, die **Du** auch erhalten möchtest,
- **Du** veröffentlichst nur Fotos und Filme, die andere auch von **Dir** machen dürfen,
- **Du** verschickst Fotos, die andere zeigen, nur wenn diese damit einverstanden sind,
- **Du** veröffentlichst nur Fotos von Dir, die **Du** auch in der Zeitung abdrucken würdest,
- **Du** lädst nur legales und erlaubtes Material herunter.

Solltest **Du** jemals diese vorgegebenen Grenzen überschritten haben, so versuche, alles was **Du** ins Netz gestellt hast, wieder zu entfernen und melde Dich persönlich bei der Person, die **Du** verletzt hast, um Dich zu entschuldigen. Zudem ist es sinnvoll, wenn **Du** Dich mit einer Person besprichst, der **Du** vertraust. Mit geeigneten Schritten kannst **Du** schlimmere Konsequenzen wie eine Strafverfolgung vielleicht abwenden oder es gelten mildernde Umstände.

Solltest **Du** bemerken, dass Freunde von Dir oder Mitglieder unserer Gruppe Cyber-Mobbing betreiben so wirke auf sie ein. Dies gilt auch für Mobbing außerhalb des Internets. Für den Fall, dass **Du** Kenntnis erlangst, dass ein(e) Freund(in) oder Bekannte(r) gemobbt wird, so helfe ihm oder ihr. Melde den Fall Deiner Schulleitung oder auch den Pastoren.

2.3 Abwehr von Cyber-Kriminalität

Kategorie: Empfehlung

Gefahrenpotential: Kapitel 1.2.3 Cyber-Kriminalität

71% aller Deutschen teilen Daten auf Facebook, die Hackern echtes Geld einbringen!!!

In diesem Kapitel geht es in erster Linie um die Straftatbestände

- Internetbetrug
- Verbreitung von Kinderpornographie
- Volksverhetzung

denen Nutzern der Facebook-Plattform ausgesetzt sind. Wir bitten Dich zu Deiner eigenen Sicherheit und zur Sicherheit Deiner Freunde und Kommunikationspartner nachfolgende Empfehlungen für Sicherheitsvorkehrungen beim Computer und Handy bzw. bei vergleichbaren Geräten der Informationstechnik zu realisieren:

- Akzeptiere auf Facebook keine Freundschaftsanfragen von Personen, die **Du** nicht kennst. Check die Personen im Zweifel auf einem anderen Weg.
- Sei vorsichtig bei Facebook-Apps, die eine zusätzliche Anmeldung bzw. Registrierung erfordern.
- Sortiere regelmäßig alte Facebook-Apps, Anwendungen und Websites aus die **Du** schon seit langer Zeit nicht mehr nutzt.
- Verwende ein starkes Passwort/Passwörter mit mindestens zehn Zeichen, Ziffern und Sonderzeichen und erneuere sie regelmäßig
- Installiere ein Virenschutzprogramm (siehe die Empfehlungen in Kapitel 3)
- Halte Deine Software auf aktuellem Stand, insbesondere den von Dir verwendeten Internetbrowser und Dein Virenschutzprogramm auf dem Computer als auch auf Deinem Smartphone.
- Benutze nie ein und dasselbe Passwort für alle Deine Anwendungen.
- Sei vorsichtig beim Klicken auf den Like-Button oder Gefällt-mir-Button. Der dahinter liegende Link könnte Dich auf eine gefährliche Abzocker-Seite leiten.

- Sperre Dein Smartphone **immer** mit einem Passwort.
- Speicher keine wichtigen Daten (Bankverbindung, PIN, Passwörter) auf dem Smartphone. Auch nicht als Mail oder SMS.
- Stimme automatischen Updates nur bei vertrauenswürdigen Apps zu.
- Solltest **Du** Dein Smartphone verkaufen oder verschenken, setze es zuvor auf die Werkseinstellungen zurück. So werden alle persönlichen Daten gelöscht.
- Wenn **Du** Dein Handy, Notebook, iPad, Tablet-PC, etc. verloren hast, solltest **Du** zunächst alle Passwörter für Online-Konten ändern, auf die **Du** mit dem Handy oder Notebook zugegriffen hast. Eventuell ist es möglich, per Remote-Zugriff auf das Handy zuzugreifen um es zu deaktivieren.
- Vorsicht beim Scannen von QR-Codes. Scanne nur vertrauenswürdige QR-Codes. Der dahinter liegende Link könnte Dich auf eine gefährliche Abzocker-Seite leiten.
- Für Zahlungen im Internet nur sichere Verbindungen verwenden, kein öffentliches WLAN[3] benutzen.
- Mails von unbekannten Absendern am besten ignorieren und auch bei neugierig machendem Betreff löschen.

QR-Code der Kirchengemeinde Victorbur

- Zip-Dateien und Links in Mails von unbekannten Absendern nicht öffnen, sie können Viren und Trojaner enthalten.
- Grobe Rechtschreib- und Grammatikfehler und abenteuerliche Geschichten in E-Mails sind ein Hinweis auf dubiose Geschäftsanbahnung.
  Hausverstand walten lassen: "Zu schön, um wahr zu sein" – was unglaublich gut klingt, ist meist auch im Internet mit einem Haken verbunden.

2.4 Verhindern der Infizierung mit Schadsoftware

Kategorie: Empfehlung

Gefahrenpotential: Kapitel 1.2.4 Infizieren mit Schadsoftware

So zeigen sich einige Anzeichen, dass Dein Computer möglicherweise mit Schadsoftware (Viren Trojaner, Würmer) infiziert wurde:

- Dein Computer läuft langsamer als normal
- Dein Computer reagiert häufig nicht oder er friert oft ein
- Dein Computer stürzt alle paar Minuten ab und startet neu
- Dein Computer startet selbsttätig neu und läuft dann nicht normal
- Anwendungen auf Deinem Computer funktionieren nicht korrekt
- Auf Laufwerke oder Festplatten kann nicht zugegriffen werden
- **Du** kannst nicht richtig drucken
- **Du** siehst ungewöhnliche Fehlermeldungen
- **Du** siehst verzerrte Menüs und Dialogfelder

[3] WLAN = Wireless Local Area Network (Kabelloses Netzwerk, Übertragung der Daten per Funk)

Dies sind gängige Anzeichen einer Infizierung - dafür können jedoch auch Hardware- oder Softwareprobleme verantwortlich sein, die nichts mit einem Virus zu tun haben. **Du** solltest ein Prüfprogramm und Entfernungsprogramm für bösartige Software installieren um in dieser Frage sicher zu sein. Siehe hierzu die Empfehlungen in Kapitel 3.

2.5 Vermeidung der Urheberrechtsverletzung

Kategorie: Richtlinie & Empfehlung

Gefahrenpotential: Kapitel 1.2.5 Verletzung des Urheberrechts

Respektiere und achte das Schaffen anderer Menschen und klaue keine geschützten Werke für Deine Zwecke. Du möchtest auch nicht wenn andere Deine Fotos oder Beiträge kopieren und unter anderem Namen verteilen oder sich damit schmücken.

- Denk daran, wenn **Du** Texte, Bilder, Videos oder Musik aus dem Internet kopierst, um diese dann in Deinem Beitrag zu verwenden, dass immer Urheber hinter diesen Dateien bzw. Werken stehen und **Du** die Eigentümer fragen müsst, ob **Du** deren Werke verwenden darfst.
  Du bist kompetent genug um selbst Texte zu schreiben oder zu fotografieren.

- Mach mit und wende Dich gegen die Urheberrechtsverletzung und das Klauen von Inhalten.

- Wirke auf Deine Freunde ein wenn **Du** merkst dass sie geklaute Texte, Bilder, Videos oder Musik mit Dir teilen wollen.

- Bekommst **Du** ein Abmahnungsschreiben in dem Dir erläutert wird, dass **Du** Dinen Rechtsverstoß gegen das Urheberrecht begangen hast regiere nicht unbedacht sondern wende Dich sofort an einen Rechtsbeistand.

3. Produktempfehlungen

In den folgenden Kapiteln findest **Du** aktuelle Produkte zur Absicherung Deines PC´s, Notebooks, Tablet-PCs und Smartphones gegen Malware. Die Aufstellung hat keinen Anspruch auf Vollständigkeit. Alle Produkte laufen im Abonnement und können verlängert werden. Im Abonnement enthalten ist das automatische Update mit aktuellen Abwehrmaßnahmen, Mustern und Eigenschaften von Trojanern und Viren, sogenannten Pattern, und aktuellen Softwareständen.

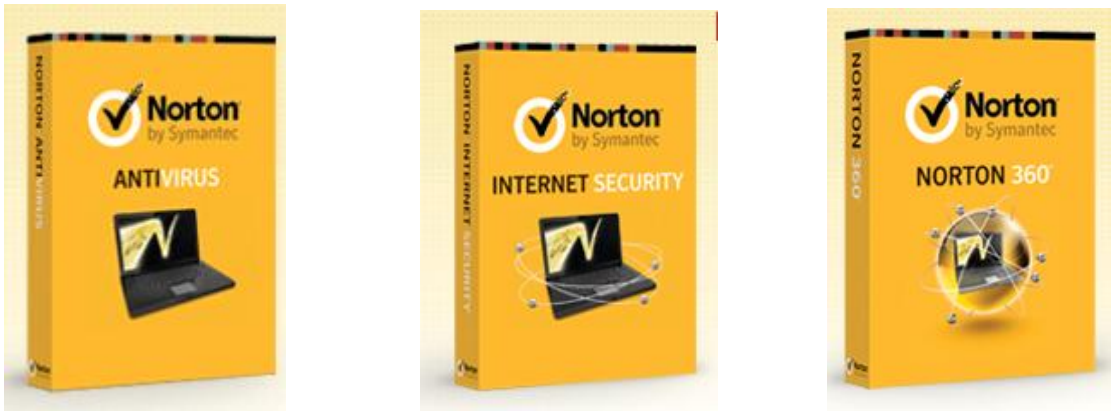
3.1 Produkte für PC und Notebook

3.1.1 Produkte der Firma Kaspersky

URL: www.kaspersky.com

3.1.2 Produkte der Firma Symantec

URL: www.**norton**.com/



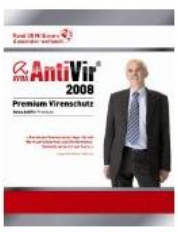
3.1.3 Produkte der Firma Avira

URL: http://www.avira.com/

AntiVir PersonalEdition... von "Avira GmbH"

Avira AntiVir... von "Avira GmbH"

15.



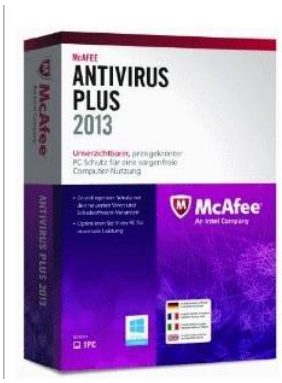
AntiVir Virenschutz 2008 V2 von "Avira GmbH"

3.1.4 Produkte der Firma GDATA

URL: http://www.gdata.de

3.1.5 Produkte der Firma Mc Afee

http://www.mcafeestore.com



Pro**Du**kte der Firma Trend Micro

URL: http://www.trendmicro.de

3.2 Produkte für mobile Geräte (Smartphones & Tablets)

Die Anzahl der Angriffe auf mobile Geräte haben sich seit dem Einsatz von Smartphones und Tablets für das Online-Banking stark erhöht sodass man auch hier auf den Einsatz von Sicherheitssoftware nicht mehr verzichten kann sofern diese Geräte für vertrauliche Kommunikation eingesetzt werden .

Siehe hierzu auch den Beitrag „*Zehn Sicherheitstipps fürs Smartphone* aus Netzwelt.
URL: http://www.netzwelt.de/news/95412-virenschutz-zehn-sicherheitstipps-fuers-smartphone.html

Siehe hierzu auch den Beitrag "*Smartphones an die Leine*" in der Computerwoche.
URL: http://www.computerwoche.de/a/smartphones-an-die-leine,2484575,7

3.2.1 Produkte der Firma Kaspersky

URL: www.kaspersky.com/de

Betriebssystem: Android

3.2.2 Pro**Du**kte der Firma F-SECURE

URL: www.f-secure.com/Mobile-Security

Betriebssystem: Android

3. 2.3 Produkt der Firma Telekom

URL: sicherheitspaket.telekom.de/

Betriebssystem: Android

3.2.5 Produkt der Firma Avira

URL: http://www.avira.com/de/avira-free-android-security

Betriebssystem: Android

AVIRA

Avira Free Android Security

3.5.6 Produkt der Firma Trend Micro

URL: http://trend-micro-mobile-security.softonic.de/windowsmobile

Betriebssystem: Microsoft Windows

3.5.7 Produkt der Firma AVG

URL: https://play.google.com/store/apps/details?id=com.antivirus&hl=de

Betriebssystem: Android

4. Querverweis