Leitfaden für den Umgang mit E-Mail und digitalen Daten

Synodalrat der Christkatholischen Kirche der Schweiz

Im Folgenden verwenden wir «@christkatholisch.ch» für die Mailadresse. Gemeint sind aber alle «Christkatholisch-Mailadressen» wie @catholique-chretien.ch, @ckjs.ch etc.

1. Warum @christkatholisch.ch?

Mit einer @christkatholisch.ch-Mailadresse unterstreichen wir, dass die Mailkommunikation geschäftlich ist und nicht von einer Privatperson kommt. Für die Arbeit in der Christkatholischen Kirche sind nur diese Adressen zu verwenden.

Wir genügen so auch aktuellen strengen Datenschutz- und Persönlichkeitsverordnungen.

2. Warum ein Mailkonto und keine Weiterleitung?

Weiterleitungen einer @christkatholisch-Mailadresse auf eine private Mailadresse sind deshalb nicht erlaubt, weil die Antwort auf ein weitergeleitetes Mail dann von einer privaten Mailadresse erfolgen würde. Somit wäre Punkt 1 nicht erfüllt.

Sie erhalten für die Arbeit in der Christkatholischen Kirche ein Mailkonto von uns zur Verfügung gestellt. Dieser Service, wie auch allfälliger Support dazu, ist für Sie kostenlos. Auf diese Weise können Sie mit der @christkatholisch-Adresse zurückschreiben.

3. Persönliche Mailadresse vs. Funktionsadressen

Persönliche Mailadressen werden an Personen vergeben; eine Funktionsadresse ist eine «unpersönliche» Adresse, bspw. «finanzverwaltung.fricktal@christkatholisch.ch». Der Vorteil von Funktionsadressen ist der, dass in Publikationen diese Adresse angegeben werden kann und bei einem allfälligen Wechsel der Finanzverwaltung, die Mailadresse dann nicht angepasst werden muss. Das Mailkonto kann ausserdem einfach der neuen Person übertragen werden und diese hat alle bisherige Korrespondenz komplett zur Verfügung.

4. Versand an alle/ BCC

Verwenden Sie bei einem Versand an viele Personen nicht die An-Funktion, sondern die BCC-Funktion Ihres Mailprogramms oder im Webmail. Alle Empfänger sehen die verwendeten Adressen im An- oder CC-Feld. Dies bringt auch allfällige Spammer auf die Idee, diese Adressen dann auch zu verwenden. Führen Sie die Empfänger im BCC auf, sind diese nicht ersichtlich. «BCC» heisst «Blind Carbon Copy» – oder «blinde Kopie».

5. Mailinglisten

Etwas anderes sind Mailinglisten: Lassen Sie sich bspw. für den Kirchgemeinderat, eine Kommission oder einen Gemeindenewsletter eine Mailingliste durch das Webteam einrichten. Sie können dann eine Mail an die Mailinglisten-Mailadresse schreiben und die Mail wird an alle in der Liste eingetragenen Mailadressen versandt. Sie können ausserdem einrichten lassen, wie eine Antwortmail verschickt werden soll (wieder an ML-Mailadressen oder an eine andere).

Bei der Verwendung einer Mailingliste als Gemeindenewsletter können sich am Newsletter interessierte Personen selbständig in die Empfängerliste eintragen. Sie erhalten auf der Webseite Ihrer Gemeinde diese Möglichkeit implementiert.

6. Webmail

Jedes Mailkonto ist selbstverständlich auch online per Webmail erreichbar. Rufen Sie die Seite https://webmail.hostpoint.ch auf und loggen Sie sich mit Ihrem Benutzernamen und dem Passwort ein. Anschliessend haben Sie Zugang auf alle Ihre Mails.

7. Mailkonto einbinden

Das Mailkonto können Sie in ihr Mailprogramm im PC/Mac oder Ihrem Smartphone einbinden. Anleitungen dazu finden Sie auf unserer Supportseite → Link (Kontaktmöglichkeiten siehe Punkt 11). Verwenden Sie für die Einbindung immer das «IMAP-Protokoll». So bleiben die Mails auf dem Christkatholisch-Mailserver und alle eingebundenen Geräte sind immer auf dem gleichen Stand.

Einmal eingebunden, können Sie dann problemlos Mails mit dem Absender @christkatholisch.ch schreiben.

Und sind Sie mal in den Ferien, blenden Sie das «Geschäftskonto» in ihrem Mailprogramm/ ihrer Mail-App während dieser Zeit einfach aus.

8. Autoresponder/ Abwesenheitsmeldungen

Alle unsere @christkatholisch-Mailkonti bieten die Möglichkeit, eine automatische Meldung an die Personen zu schicken, die Ihnen eine Email schreiben. Einrichten können Sie dies, wenn Sie sich online via Webmail in Ihr Mailkonto einloggen (siehe Punkt 6).

9. Spam

Leider ist auch unsere Mail-Infrastruktur nicht vor Spam gefeit. Wir arbeiten eng mit unserem Webhoster (Hostpoint) zusammen und versuchen, möglichst viele der Spammails auszufiltern. Leider sind die Spammer immer «gewiefter» und versuchen mit immer neueren Methoden, ihre unerwünschten Nachrichten zu verbreiten.

Im Mailkonto werden Spammails in der «Spambox» abgelegt und automatisch nach 3 Tagen gelöscht.

Beachten Sie zu diesem Thema auch die weiterführenden Informationen in Punkt 12.2.

10. Passwortmanagement

Verwenden Sie für alle Ihre Onlinekonti ein separates, eigenes Passwort. Mit Onlinekonti sind nicht nur Mailkonti gemeint, sondern auch alle Ihre Konti bei Versandhändlern, Sozialen Medien etc. im Internet.

Damit Sie den Überblick behalten, gibt es sogenannte Passwortmanager-Programme bzw. -Apps (bspw. KeePass etc.). Diese Passwortmanager speichern alle Passwörter, welche Sie zum Einloggen auf beliebigen Webseiten benötigen und sind über ein Master-

Passwort geschützt. Die Manager helfen auch bei der Generierung von sicheren Passwörtern.

Eingebunden in Ihrem Browser (Firefox, Chrome etc.) tragen diese Manager dann das entsprechende Passwort beim Login automatisch ein. Sie brauchen sich also nur noch das Master-Passwort zu merken.

11. Kontakt zum Webteam/ Hilfestellungen

Haben Sie eine Frage oder ein Anliegen, können Sie sich gerne ans Webteam mit der Mailadresse support@christkatholisch.ch wenden.

Ebenfalls finden Sie online Hilfe auf unserer Supportseite unter https://christkatholisch.ch/support

12. Weitere hilfreiche Tipps zu E-Mail, Internet und Passwörtern

12.1 Passwort-Management

1. Die Passwörter von sämtlichen E-Mail-Accounts sollten mindestens einmal im Jahr, allerdings nicht zum selben Zeitpunkt, gewechselt werden.

2. Neue Passwörter sollten (Stand 2019) eine Länge von mindesten 8 Zeichen aufweisen.

3. Diese Zeichenfolge sollte, falls technisch möglich, zusammengesetzt sein aus Gross- und Kleinbuchstaben, Sonderzeichen (/ -!+? etc.) sowie Zahlen.

4. Zeichen sollten sich innerhalb eines Passworts nicht wiederholen («555222nN===» wäre ein schwaches Passwort).

5. Passwörter sollten an einem verlässlichen Ort notiert werden.

    1. Falls hierfür ein digitales Dokument verwendet wird, dann sollte sich dieses nicht auf einem Computer mit Internetanschluss befinden, sondern z.B. auf einer externen Festplatte oder einem USB-Stick, welcher nur an den Computer angeschlossen wird, nachdem dieser vorübergehend vom Internet getrennt wird.

    2. Alternativ dazu kann eine Passwort-Management-Software verwendet werden, welche Passwörter enthält und diese bei Bedarf automatisch in Browser-Login-Seiten einträgt (Z.B. KeePass).

    3. Das «Master»-Passwort dieser Software sollte speziell sicher gewählt sein.

12.2 Nachrichten-Management

1. Aus Sicherheitsgründen sollten nur E-Mail geöffnet werden, welche von einem «vertrauenswürdigen» Absender kommen.

2. Beim Absender eines E-Mails sollte überprüft werden, ob der angezeigte Name im Kopfteil des E-Mails (z.B. «CHK Webmaster») tatsächlich mit der rechts davon angezeigten E-Mailadresse (z.B. «webmaster@christkatholisch.ch») übereinstimmt. SPAM-Mails enthalten oft gefälschte

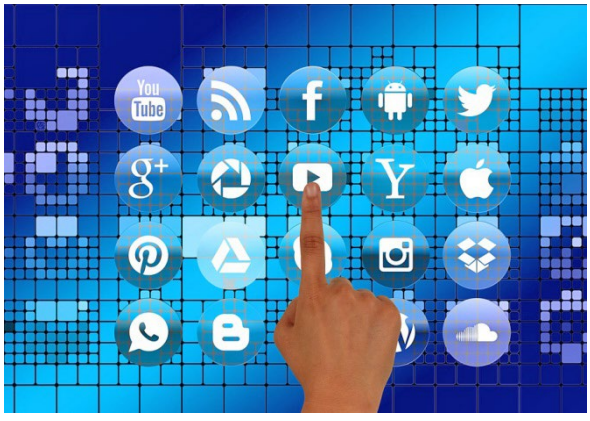
Namen (z.B. auch «Vorname.Nachname@christkatholisch.ch). Rechts davon steht als realer Absender allerdings die reale Adresse des SPAM-Autors (z.B. «conem@infoflood.co.uk»).

3. SPAM-Mails sollten nicht einfach gelöscht werden, sondern, wenn möglich, zuerst im Mailprogramm als SPAM markiert und erst dann, z.B. im SPAM-Ordner, gelöscht werden. So wird dem E-Mail-Programm ermöglicht, dazu zu lernen und SPAM-Mails mit der Zeit immer besser zu erkennen.

4. Anhänge in E-Mails sollten idealerweise zuerst auf dem Computer gespeichert und erst dann geöffnet werden. So wird der Sicherheits-Software auf dem Computer ermöglicht, den Anhang beim Öffnen zu prüfen.

12.3 Sicherheits-Status

Über das Internetportal https://haveibeenpwned.com kann überprüft werden, ob und wann eine Emailadresse bei einem Datenleck von Hackern aus einer geschützten Datenbank (z.B. bei einem Online-Shop) «erbeutet» werden konnte. Sollte dies kürzlich geschehen sein, empfiehlt es sich dringend, das Passwort für den entsprechenden Online-Shop zu ändern.



12.4 Internet

1. Installieren Sie unbedingt einen Virenscanner auf Ihrem Computer! Diese Virenscanner durchsuchen die heruntergeladenen Programme auf Viren und Schadsoftware. Regelmässige Updates des Virenscanners gehören natürlich auch dazu.

2. Downloads aus dem Internet sind prinzipiell potenziell gefährlich. Heruntergeladene Dateien oder Ordner können bei Bedarf nach dem Download auch mit einem Online-Virenprüfer auf Sicherheitsprobleme geprüft werden (z.B. https://www.virustotal.com). Dort wird eine Datei mit über 50 verschiedenen, stets aktuellen Antivirus-Programmen auf Probleme geprüft. Hierfür muss die zu prüfende Datei allerdings zum Prüfer hochgeladen werden. Folglich sollten keine privaten Daten auf diese Weise geprüft werden.

3. Webseiten können von Hackern attackiert worden sein. Um sicher zu gehen, dass es sich bei einer mittels Internet-Adresse (z.B. «www.christkatholisch.ch») aufgerufenen Internetseite tatsächlich um die gewünschte Seite handelt, kann bei Internet-Adressen, welche mit «https» beginnen, auf die Information zum Sicherheits-Zertifikat (im Browser links der Internet-Adresse) geklickt werden. Dort finden sich u.a. Informationen zum «Besitzer» des Sicherheitszertifikats. Weichen diese Informationen stark von den Angaben des vermuteten Betreibers der Seite ab, könnte die Seite «gehackt» worden sein.

4. Über die Internetadresse https://www.whois.com können Informationen zum Betreiber bzw. Besitzer einer Internetseite abgerufen werden.