E-Mail

Verbindung mit mobilen Geräten

umgezogen nach https://wiki.ph-freiburg.de/!service/email:mobilgeraet

Mailinglisten

umgezogen nach https://wiki.ph-freiburg.de/!service/email:mailinglisten

Webschnittstelle Horde

umgezogen nach https://wiki.ph-freiburg.de/!service/email:horde

Lesezeichen speichern

- Unter dem Menüpunkt „Weitere\Lesezeichen“ können Lesezeichen angelegt und verwaltet werden.

E-Mail-Client einrichten

Thunderbird-Anleitung

umgezogen nach https://wiki.ph-freiburg.de/!service/email:thunderbird

Sicherheit bei der Nutzung von E-Mail

umgezogen nach https://wiki.ph-freiburg.de/!service/email:sicherheit

Zertifikat in E-Mailprogramm einrichten

Beschreibung für Horde: umgezogen nach https://wiki.ph-freiburg.de/!service/email:horde#s_mime_zertifikat In Thunderbird klicken Sie auf Extras → Konten-Einstellungen → Ende-zu-Ende-Verschlüsselung.

- Nun auf „S/MIME-Zertifikate verwalten“ klicken.
- Im geöffneten Fenster „Zertifikatverwaltung“ kann das Zertifikat importiert werden. Dabei wird nach einem Kennwort gefragt. Hierfür verwenden Sie bitte das gleiche Kennwort welches Sie

beim Sichern der Zertifikatsdatei genutzt haben.
- Nach dem das Zertifikat importiert wurde, kann dieses über den „Auswählen…“-Button ausgewählt werden.
- Danach werden Sie gefragt, ob das Zertifikat auch zum Ver- und Entschlüsseln verwendet werden soll. Hier wählen Sie bitte „Nein“ aus.
- Nach diesem Schritt noch den Haken bei „Eigene digitale Unterschrift standardmäßig hinzufügen“ setzen

IMAP/SMTP Daten PH-Freiburg

- Post**ein**gangsserver: IMAP, Serveradresse: imap.ph-freiburg.de, Port: 993 mit SSL
- Post**aus**gangsserver: SMTP, Serveradresse: smtp.ph-freiburg.de, Port: 465 mit SSL oder Port 587 und 25 mit StartTLS

Es werden nur E-Mails zum Versand angenommen, wenn die darin verwendete Absenderadresse Ihrem Login zugeordnet werden kann.
Sollte ihr Mailprogramm einen Authentifizierungstyp erfragen, so verwenden sie bitte PLAIN.

Als Login/Benutzername ist ihr PH-Login (z.B. muellerfr/xyz123) anzugeben.

Wichtig: Bei SMTP muss ebenfalls Login und Kennwort verwendet werden.
Andernfalls könnten sie nur E-Mails an unsere eigene Maildomain richten (Beispiel: support@ph-freiburg.de klappt, support@gmx.de kommt mit Fehler „relay access denied“ zurück).

IMAP-Ordner freigeben

In der Mail-Komponente von Horde können IMAP-Ordner folgendermaßen für andere Hochschulmitglieder freigegeben werden:
- einen Rechtsklick auf den betreffenden Ordner
- dann auf „ACL bearbeiten“,.
- dann den Login eintragen,
- dann dort im Pulldown wo „Vorlagen:“ steht idR „Alle“ Rechte vergeben und dann
- unten auf „Speichern“ klicken.

Funktionsadresse, kooperatives Arbeiten

Die PH bietet folgende Möglichkeiten des kooperativen Arbeitens über Funktionsadressen an:

1. Alias
Eine Alias-Adresse ist eine (Funktions-) E-Mail Adresse, die Ihrem und ggf. weiteren PH-Accounts zugeordnet werden kann.
E-Mails an diese Adresse werden allen Personen mit dieser Alias-Adresse zugestellt.

2. Gruppenmailbox
Eine Gruppenmailbox ist ein spezielles Postfach mit eigener E-Mail-Adresse, welches mit Ihrem und weiteren PH-Accounts verknüpft werden kann.
Über Horde können zugeordnete Nutzer der Gruppenmailbox auf ein gemeinsames Postfach zugreifen (Einbindung in externes Mailprogramm ist nicht möglich).

Die Nutzer der Gruppenmailbox können von einem Verantworlichen (Moderator) über einen Service im ZIK-Portal verwaltet werden.

3. Mailing-Liste
Eine Mailingliste bietet einem geschlossenen Personenkreis die Möglichkeit des Nachrichtenaustauschs.
Sie besteht aus einer Liste von E-Mail-Adressen, die selbst eine E-Mail-Adresse in der Form [listenname]@lists.ph-freiburg.de hat.
Nachrichten an diese Adresse werden allen Mitgliedern der Mailingliste an die eingetragene E-Mail-Adresse weitergeleitet.
Unsere Mailinglistensoftware (mailman) läßt sich über ein Webinterface dabei so einstellen, dass entweder alle Mitglieder direkt Nachrichten an diese Liste verschicken dürfen,
der Moderator jede Nachricht der Mitglieder an die Liste freigeben muss (moderierte Liste) oder,
dass nur der Moderator der Mailingliste selbst das Recht hat Nachrichten an die Mitglieder der Liste zu versenden (Newsletter).

Falls Sie Bedarf an einer Funktionsadresse / Mailingliste haben und / oder kooperativ mit anderen Personen arbeiten möchten, schreiben Sie unter Angabe der Wunschadresse und ggf. der beteiligten Personen eine E-Mail an support@ph-freiburg.de, wir finden dann gemeinsame mit Ihnen die beste Lösung.

Gruppenmailbox

Da es sich bei der Gruppenmailbox auch um eine Hordeinstanz handelt, welche im Browser geöffnet wird, gibt es einen kleinen Workaround,
falls schon eine Hordeinstanz (über pmail / smail) geöffnet wurde. (Ist dies nicht der Fall, können Sie ab Punkt 3 beginnen)

1. Firefox öffnen und oben rechts auf (Menü öffnen) klicken
2. „Neues privates Fenster“ auswählen
3. Horde (https://pmail.phfr.de) in einem (neuen, privaten) Fenster öffnen
   Auf „LogIn Gruppenmailbox“ klicken
4. Anmelden (Benutzername + Kennwort des zugeordneten Accounts)
5. Falls mehrere Gruppenmailboxen vorhanden sein sollen, wählen die entsprechende Gruppenmailbox aus.

Sind Sie der erste Nutzer, der sich an der Gruppenmailbox anmeldet, gehen Sie bitte wie folgt vor:

1. Einstellungen (Zahnrad) → Benutzereinstellungen → Webmail anklicken
2. Persönliche Angaben anklicken
3. Unter Standardidentität Namen, Standard-E-Mail (optional: Signatur) einpflegen
4. Speichern
5. Nun erhalten Sie eine E-Mail, in der Sie Ihre Identität bestätigen müssen (Link anklicken)
6. Daten kontrollieren und „Speichern“
7. Die Ersteinrichtung ist nun abgeschlossen

Falls Sie ein Gruppenmailzertifikat benötigen, können Sie sich gerne an support@ph-freiburg.de wenden.

Per Alias Mail verschicken

Nachdem für Sie beim Helpdesk ein Alias eingerichtet wurde, empfangen Sie die Mails der Aliasadresse.
Um unter der neuen Alias schreiben zu können, erstellt man im Mailclient ein weiteres Profil.

Dabei geht man folgendermaßen vor:

1. In Horde auf Zahnrad\Benutzereinstellungen\Webmail\Persönliche Angaben klicken
2. Unter „Wählen Sie eine Identität“ „Neue Identität anlegen“
3. Entsprechende Angaben tätigen. Wichtig ist, unter „Die Standard-E-Mail-Adresse für diese Identität:“ Ihren (neuen) Alias einzutragen
4. Speichern
5. Sie bekommen eine E-Mail, die bestätigt werden muss. (evtl. im SPAM-Ordner nach der Bestätigungs-Mail nachschauen)
6. Danach können Sie in Horde bei „Neue Nachricht“ unter „Von“ die zweite Identität auswählen

Falls Sie Thunderbird verwenden, finden Sie unter folgendem Link eine Anleitung:
https://support.mozilla.org/de/kb/identitaeten-verwenden

Abwesenheitsnachricht per Horde

Am besten können Sie die Abwesenheitsnachricht über Horde einrichten, das geht wie folgt ganz einfach.

1. Horde öffnen und anmelden
2. Auf „Webmail“ gehen nun „Filter“ auszuwählen.
3. Dies führt Sie zu den „Filterregeln“
4. Das Wort „Abwesenheit“ anklicken
5. Dort können Sie Beginn und Ende der Nachrichten, denn Betreff der E-Mail und auch den Inhalt (Grund) angeben.
6. Auf „Erweiterte Einstellungen“ klicken (oberhalb des Punktes „Beginn der Abwesenheit“)
7. Dort Ihre Mailadresse (Meine E-Mail-Adresse) angeben

8. Speichern und Aktivieren klicken
9. Nun ist die Abwesenheitsmail für den angegebenen Zeittraum aktiv.

Gemeinsam genutzter Horde-Kalender erstellen

1. In Horde anmelden und zu „Kalender“ navigieren
2. Neben „Meine Kalender“ klicken Sie bitte das Plus-Symbol an, um einen (weiteren) Kalender zu erstellen.
3. Eine aussagekräftigen Kalendernamen verwenden und die gewünschte Farbe auswählen
4. Zu „Teilen“ navigieren
    1. Hier können Sie, durch einen Klick auf „Mit den Benutzern:“, im unteren Feld die Logins der zu berechtigten Personen eintragen.
    (Das Format der Benutzernamen bei alten Logins ist z.B. musterfraufr und bei den Neueren z.B. abc123 / Studierende-Accounts können nicht berechtigt werden)
    Durch eine kommagetrennte Eingabe von Benutzernamen können Sie mehrere Personen berechtigen, wie z.B.: musterfraufr, abc123, xyz789
    2. Im nächsten Schritt vergeben Sie jeweils die Berechtigungen, was eine Person darf. Die Standardeinstellung ist „Termine zu lesen“
    In diesem Fall kann nur der/die Ersteller*in Termine hinzufügen. Bei „Termine zu lesen und zu bearbeiten“ darf jede der oben aufgeführte Benutzer*in Termine lesen/erstellen.
    3. Wenn Sie möchten das die freigegebene Person auch Termine löschen kann. Klicken Sie auf „Erweiterte Rechte-Einstellungen“ und setzen Sie dann den Haken bei Löschen.
5. Nach dem Klick auf „Speichern“ wird der Kalender erstellt
6. Der/Die Ersteller*in sieht nun den neuen Kalender unter „Meine Kalender“. Über das Stiftsymbol kann der Kalender bearbeitet werden.
7. Die berechtigten Benutzer*innen sehen nun den neuen Kalender unter „Gemeinsame Kalender“. Standardmäßig ist dieser eingeklappt und wird über das Dreiecksymbol auf der linken Seite sichtbar.
8. Um den gemeinsamen Kalender in der Ansicht (parallel zum eigenen) anzeigen zu lassen, setzen Sie den den entsprechenden Haken vor den Benutzer*innen.
9. Durch den Klick auf „Neuer Termin“ oder in den Kalender, erstellen Sie einen Termin. Soll dieser nun für alle Benutzer*innen gelten, wählen Sie bei „Termin hinzufügen zu:“ den gemeinsamen Kalender aus.
10. Zuletzt müssen Sie den Termin noch „Speichern“.

Gemeinsam genutzter Horde-Mailordner

1. In Horde anmelden und zu „Webmail“ navigieren
2. Rechtsklick auf den Ordner, den Sie freigeben möchten
3. „ACL bearbeiten“ klicken
4. Nun können Sie bei Benutzer den PH-LogIn der Person eingeben, die die Zugriffsberechtigung erhalten soll
5. Mit der Vorlage können Sie verschiedene Vorlagenmodelle auswählen oder individuell setzen, welche Berechtigungen die Person bekommen sollen.
6. Speichern klicken

Ordner bei Kollege*Innen

1. In Horde unter Webmail „Ordneraktionen“ anklicken
2. „Alle Ordner anzeigen“ auswählen
3. Der freigegebene Ordner wird nun unter „user“ → „LogIn des Besitzers angezeigt

Dienstliche Daten und persönliche Schlüssel/Zertifikate

Wenn Sie dienstliche Daten verschlüsseln und dabei Ihr persönliches Zertifikat verwenden, können nur Sie und nicht Ihr Dienstherr auf die Daten zugreifen. Bei Verlust des Schlüssels, bei Todesfall, wenn Sie sich weigern oder nicht verfügbar sind o.a., kann der Dienstherr nicht mehr auf die dienstlichen Daten zugreifen.

Daher sollten dienstliche Daten, welche zu einem späteren Zeitpunkt nochmals verwendet werden sollen, nicht mit einem persönlichen Zertifikat verschlüsselt werden.

Als Alternative kann sich unter Umständen ein Gruppenzertifikate anbieten, doch auch hier gibt es Risiken: Scheiden Personen aus der Gruppe aus und hatten direkten Zugriff auf die Zertifikatsdaten mit dem privaten Schlüsseln, muss ein neues Zertifikat mit neuem Schlüsseln für diese Gruppe erstellt werden. Die alten Dokumente können aber nur mit altem Schlüssel gelesen werden. Das Schlüsselmanagement muss diesen Anforderungen gerecht werden können.

Verschlüsselung nur für eingeschränkten Nutzerkreis möglich

Bei der Verschlüsselung wird durch das Mailprogramm der Nachrichtentext zweimal, mit zwei verschiedenen, öffentlichen Schlüsseln verschlüsselt. Einmal mit dem eigenen Public Key, damit man die Korrespondenz selbst noch lesen kann und einmal mit dem Public Key des Empfängers. Daher gilt:

Nur wenn der Public Key des Empfängers vorliegt, wenn der Empfänger also selbst ein S/MIME Zertifikat hat, kann dieser die verschlüsselte Nachricht entschlüsseln und lesen.

Schlüsselverwaltung mehrerer Generationen, Verlust des Schlüssels

Prüfen und klären Sie vorab, ob und wie Ihr verwendetes Mailprogramm mit mehreren, oder alten, abgelaufenen Zertifikaten/Schlüsseln umgehen kann. Denn ein Zertifikat ist nur für eine begrenzte Zeit gültig. Danach muss es erneuert werden. Oft werden hierbei ebenso die Schlüsselpaare erneuert. Sie können auf alte, verschlüsselte Daten nur zugreifen, wenn Ihr Mailprogramm die passenden, alten Schlüssel vorhalten kann und installiert hat. Wird der Schlüssel verloren (z.B. durch Schaden o. Verlust des PCs) und ist keine Sicherung vorhanden, oder wird das Passwort zum Schutz des Schlüssels vergessen, sind die verschlüsselten Daten unwiederbringlich verloren.

Betrug, fälschliche Sicherheit und Virenscanner

Ein Angreifer, ein Betrüger ein „Spammer“ kann Ihnen eine verschlüsselte und signierte E-Mail zuschicken. Er könnte hierfür mit einem gestohlenen Zertifikat unterschreiben, bzw. sich an verschiedenen Stellen selbst eines besorgt, erstellt haben. Signierte und verschlüsselte E-Mails können ebenso SPAM und Viren beinhalten!

Wenn Sie eine verschlüsselte E-Mail empfangen haben, kann kein Virenscanner zuvor einen etwaigen Virus in dieser E-Mail erkennen. Bis zum Zeitpunkt der Entschlüsselung bleibt völlig unklar, was für Daten in der E-Mail enthalten sind. Sie sollten sich deshalb nicht in fälschlicher Sicherheit wiegen, wenn Sie eine signierte und auch noch verschlüsselte E-Mail erhalten. Es gilt hier besonders, die E-Mail auf Plausibilität, auf ein gültiges Zertifikat hin zu prüfen und Dateianhänge nicht blind links zu öffnen.

Prüfen Sie genau den Absender, das dort verwendete Zertifikat. Trauen Sie nicht „blind“ signierten, besonders nicht noch verschlüsselten, E-Mails.

Inkompatibilitäten von Mailprogrammen

Die Entwicklung der Mailprogramme durch die verschiedenen Hersteller gewährt nicht immer, dass Technologien in allen Programmen gleich, bzw. überhaupt, vorhanden sind. Bevor ein Prozess auf verschlüsselte Mailkommunikation zwischen zwei Stellen festgelegt wird, ist zu prüfen und zu testen, ob die Gegenstellen problemlos Ihre Daten lesen und verarbeiten können. Bedauerlicherweise ist die Technologie S/MIME nicht in allen Mailprogrammen realisiert. Es sind auch Probleme zwischen unterschiedlichen Mailprogrammen mit S/MIME Unterstützung bekannt. Die Probleme könnten in zukünftigen Versionen behoben sein, aber auch erst noch auftauchen.