

# Newsletter des Rechenzentrums

## Ausgabe April 2020

### Inhalt:

1. Brief des CIO zu Maßnahmen in der Corona-Krise / Fair Share-Aufruf
2. Homeoffice in der Corona-Krise
3. Sichere IT-Nutzung im Homeoffice
4. Digitale Lehre im Sommersemester
5. Onlineberatung zu IT-Schulungsthemen
6. Neue Passwortregeln erfordern Handeln der Benutzer
7. Was tun bei Phishing-Mails?
8. Neuer FTP-Server in Betrieb genommen
9. Der IT-Support fragt nie nach Passwörtern!

***Die Corona-Pandemie hat natürlich auch unseren Newsletter durcheinandergewirbelt. Sicherlich wird die Krise auch noch in den nächsten Wochen und Monaten für ein ungewöhnliches Sommersemester an der JMU sorgen. Trotzdem oder gerade deswegen finden Sie in diesem Newsletter zahlreiche Tipps und Hinweise, wie Sie einerseits auch im Homeoffice effektiv arbeiten und andererseits Lehren und Lernen im nahenden Semester so gut wie möglich absolvieren können. Wir wünschen allen Lesern Frohe Ostern und – bleiben Sie gesund!***



## **1. Brief des CIO zu Maßnahmen in der Corona-Krise / Fair Share-Aufruf**

Der CIO der Universität Würzburg zu den bisher ergriffenen Maßnahmen in der Corona-Krise aus IT-Sicht. (Also available in English)

Sehr geehrte Damen und Herren,

aufgrund der aktuellen Situation möchte ich Sie hiermit über die begonnenen Maßnahmen zur Verbesserung der Möglichkeiten in Bezug auf die Forschung, Verwaltung und Lehre von außerhalb der Universität informieren. Da trotz der zahlreichen ergriffenen Maßnahmen viele (digitale) Ressourcen knapp sind, möchte ich Sie **auch um die Einhaltung verschiedener „Fair Share Regeln“ bitten.**

### **BITTE LEITEN SIE DIESE INFORMATIONEN ENTSPRECHEND WEITER!**

**Telefonische Erreichbarkeit:** Sie können Ihr dienstliches Telefon auf eine Rufnummer außerhalb der Universität weiterleiten. Dieses geht über [diesen](#) Link. Zur Einrichtung benötigen Sie eine VPN-Verbindung (bitte trennen Sie immer Ihre VPN-Verbindung, wenn Sie diese nicht mehr benötigen). Die Anzahl der in die Universität eingehenden Telefonverbindungen ist begrenzt. Wir möchten Sie daher bitten, interne Gespräche über die angebotene Alternative „Microsoft Teams“ zu führen, um die Leitungen für eingehende Gespräche von extern freizuhalten. Alternativ schlagen wir, vor, dass Sie mit Gesprächspartnern, mit denen Sie häufiger telefonieren die Telefonnummern austauschen und sich direkt anrufen.

**Sitzungen und Teambesprechungen:** Sie benötigen für keinen der hier genannten Video-oder Chat-Dienste (DFN Conferencing, Teams, Rocket Chat, Jitsi) VPN – bitte trennen Sie die VPN-Verbindung, wenn Videokonferenzen nutzen! Für Sitzungen und Teambesprechungen steht der Dienst des DFN (DFNConf) zur Verfügung. Dieser hat aufgrund der verstärkten Nutzung in der aktuellen Krise insbesondere zu Peak-Zeiten Lastprobleme, bitte versuchen Sie (sofern möglich) Besprechungen außerhalb der [Spitzenzeiten](#) anzusetzen.

Als Alternative gibt es seit kurzer Zeit die Möglichkeit, [Microsoft Teams](#) zu nutzen. Eine Aktivierung ist über [Studisoft](#) (dort Produkte-Microsoft) möglich. Bitte beachten Sie die

Informationen zur Datenverarbeitung. Mit Teams können Sie Telefonkonferenzen und Videokonferenzen abhalten, wir empfehlen, die Nutzung weiterer Funktionen (z.B. Chat) zu unterlassen und stattdessen auf die datenschutzrechtlich unbedenklichen vorhandenen Tools (z.B. Email, WueTeams etc.) zurückzugreifen. Eine dauerhafte Bereitstellung von Teams für die Zeit nach der Corona-Krise kann nicht zugesichert werden, dort gespeicherte Daten werden auch nicht gesichert. Bitte haben Sie Verständnis dafür, dass wir keinen Support für Teams anbieten können, Sie haben aber in [WueCampus](#) die Möglichkeit, mit anderen Benutzern Fragen zum Produkt und zur Verwendung zu diskutieren.



Abbildung 1: CIO der JMU, Matthias Funken (Foto: privat)

Ab April werden wir zusätzliche Dienste im Rechenzentrum in Betrieb nehmen: Mit Rocket Chat können Sie datenschutzrechtlich unbedenklich chatten, mit Jitsi sind ebenfalls Videokonferenzen möglich. Wir führen diese Dienste auch ein, um einen (begrenzten) Fallback zu haben, sollten die öffentlich verfügbaren Systeme aufgrund der weltweiten Pandemie Stabilitätsprobleme bekommen. Auch für diese Systeme können wir aktuell keine dauerhafte Verfügbarkeit für die Zeit nach der Krise zusichern.

**Virtual Private Network (VPN):** Die Anzahl der VPN-Verbindungen in die Universität ist begrenzt, reicht aber bei geöffneter Bibliothek, zugänglichen CIP-Pools und normalem Vorlesungsbetrieb in der Universität bei weitem aus. Ein Hochskalieren des Dienstes ist kurzfristig u.a. aufgrund von nicht lieferbarer Hardware nur in sehr eingeschränktem Umfang möglich und wird vermutlich in der ersten April-Woche erfolgen. Auch danach stellt VPN eine sehr knappe Ressource dar, daher bitten wir Sie um eine faire Nutzung: Bitte trennen Sie grundsätzlich Ihre VPN-Verbindung, wenn Sie diese nicht benötigen. Viele Dienste der Universität benötigen kein VPN, bitte versuchen Sie vor einem Verbindungsaufbau, ob der Dienst nicht auch ohne VPN-Verbindung erreichbar ist.

- Netzlaufwerke erreichen Sie mit einem Browser über den Dienst [Files](#).
- Video-Konferenz-Dienste wie DFN, Zoom, Jitsi oder Microsoft Teams benötigen grundsätzlich keine VPN-Verbindung.
- Viele [Inhalte](#) der Bibliothek sind auch ohne VPN erreichbar
- [Hier](#) finden Sie eine Übersicht über die Dienste, für die Sie VPN benötigen

**Vorlesungsübertragung (live):** Für die Übertragung von Vorlesungen werden wir ab der ersten April-Woche hinreichend viele Lizenzen der Software „Zoom“ zur Verfügung stellen. Auch für Zoom werden wir in WueCampus eine Diskussionsgruppe eintragen. Für die Verwendung von Zoom benötigen Sie ebenfalls kein VPN. Weitere Informationen finden Sie [hier](#), eine Kurzanleitung finden Sie [hier](#).

**Unterlagen, Screencasts, Videos, eLearning:** Selbstverständlich steht Ihnen unsere eLearning-Plattform WueCampus zur Verfügung. WueCampus wurde mit zusätzlichen Hardware-Ressourcen ausgestattet, um den erwarteten Upload von Lehrmaterialien managen zu können. Allerdings bitten wir auch hier um Ihre Mitarbeit: Versuchen Sie, die in WueCampus hochgeladenen Dateien klein zu halten. Für die mediale Anreicherung von Inhalten schlagen wir z.B. die Verwendung von Audiospuren in Powerpoint vor, was zu wesentlich kleineren Dateien im Vergleich zu Videoaufzeichnungen von Vorlesungen führt. (Siehe hierzu auch die Webseite „[Lehre Digital](#)“.

Zur Erstellung von Screencasts stehen zusätzliche [Camtasia](#)-Lizenzen im Webshop zur Verfügung. Zur Erstellung von Videos im Home Office braucht es nicht viel, ein paar Tipps finden Sie [hier](#).

In begrenztem Umfang haben wir auch für das kommende Semester wieder Slots für reguläre Vorlesungsaufzeichnungen zur Verfügung gestellt. [In 13 fest definierten Hörsälen kann eine Aufzeichnung reserviert werden.](#)

Zusätzlich haben wir ab Anfang April einige Räume im zentralen Hörsaal- und Seminargebäude (Z6) für Sie mit „Aufnahmeequipment“ ausgestattet. Dort können Sie in Eigenregie Aufzeichnungen erstellen sowie Audiounterlegung von Powerpointfolien durchführen. Anleitungen für die Geräte sind vorhanden, außerdem gibt es bei Bedarf auch einen Online-Support. Mehr Informationen zu diesem Angebot finden Sie [hier](#), eine Reservierung dieser Räume im Z6 ist [hier](#) möglich.

Für die Bereitstellung von Aufzeichnungen, Videos und Screencasts steht Ihnen der Dienst „Lecture“ zur Verfügung. Aufgrund der erwarteten Menge von Videos werden wir gegen Ende April einen weiteren in WueCampus integrierten Video-Streaming-Server bereitstellen, der zusätzliche Kapazität für die Bereitstellung von Videos zur Verfügung stellt.

Von einem Upload zu Youtube möchten wir aus datenschutzrechtlichen Gründen abraten, solange die hier aufgezeigten Alternativen performant zur Verfügung stehen. Die dort abgelegten Medien sind grundsätzlich immer weltweit frei verfügbar und können nicht für eine bestimmte Nutzergruppe eingeschränkt werden!

**Softwareangebot:** Durch die aktuellen Maßnahmen zur Eindämmung des Coronavirus und die damit verbundene Schließung der Universität Würzburg, haben sich einige Erweiterungen des Softwareangebots auf [Studisoft.de](#) ergeben. Einzelheiten zur Erweiterung sind der [Liste Softwareprodukte](#) zu entnehmen.

Auch wenn wir in den letzten Wochen viel unternommen haben, um die Universität für Forschung, Lehre und Verwaltung in den nächsten Wochen vorzubereiten, bleiben die technischen Ressourcen sehr begrenzt. Sie können einen wesentlichen Beitrag dazu leisten, dass der Betrieb vieler Prozesse für alle aufrechterhalten werden kann. Dafür möchte ich mich schon jetzt bei Ihnen bedanken.

Mit freundlichen Grüßen,  
 Matthias Funken

Alle Maßnahmen nochmals als Shortcuts:

<https://www.rz.uni-wuerzburg.de/aktuelles/mitteilungen/single/news/homeoffice-fuer-forschung-und-lehre-in-zeiten-von-corona/>

ENGLISH VERSION:

To whom it may concern,

due to the current situation, I would like to inform you about the measures taken to improve the possibilities for research, administration and teaching from outside the university. As many (digital) resources are scarce despite the numerous measures taken, I would also like to ask you to observe various "fair share rules".

**Reachability by telephone:** You can forward your business telephone to a number outside the university. This can be done via [this](#) link. You will need a VPN connection to set it up (please always disconnect your VPN connection when you no longer need it). The number of telephone connections coming into the university is limited. We would therefore ask you to make internal calls via the offered alternative "Microsoft Teams" to keep the lines free for incoming calls from outside. Alternatively, we suggest that you exchange telephone numbers with people you frequently call and call each other directly.

**Sessions and team meetings:** You do not need VPN for any of the video or chat services mentioned here (DFN Conferencing, Teams, Rocket Chat, Jitsi) - please disconnect the VPN connection if you use video conferencing! For sessions and team meetings the service of DFN (DFNConf) is available. Due to the increased use in the current crisis, this service has load problems, especially at peak times. Please try to schedule meetings outside [peak times](#) (if possible).

As an alternative, [Microsoft Teams](#) has recently been made available. Activation is possible via [Studisoft](#) (there products - Microsoft). Please note the information on data processing. With teams you can hold telephone conferences and video conferences. We recommend that you refrain from using other functions (e.g. chat) and instead use the existing tools (e.g. email, WueTeams etc.) which are not subject to data protection laws. A permanent provision of teams for the time after the Corona crisis cannot be guaranteed, nor will data stored there be backed up. Please understand that we cannot offer support for teams, but in [WueCampus](#) you have the opportunity to discuss questions about the product and its use with other users.

Starting in April, we will start to offer additional services in the computer center: With Rocket Chat you can chat without any data protection concerns, Jitsi will provide on-

site video conferencing. We are also introducing these services to have a (limited) fallback should the publicly available systems get stability problems due to the worldwide pandemic. Also for these systems we can currently not guarantee permanent availability for the time after the crisis.

**Virtual Private Network (VPN):** The number of VPN connections to the university is limited, but would be by far sufficient with an open library, accessible CIP pools and normal lecture operations at the university. An upscaling of the service is only possible to a very limited extent in the short term due to non-available hardware, among other things, and will probably take place in the first week of April. Even after that, VPN is a very scarce resource, so we ask you to use it fairly: **Please always disconnect your VPN connection if you do not need it.** Many services of the university do not require VPN, please try before establishing a connection to the university to see if the service is not accessible without a VPN connection.

- Network drives can be accessed with a browser via the service [Files](#).
- Video conferencing services such as DFN, Zoom, Jitsi or Microsoft Teams generally do not require a VPN connection.
- Many [contents](#) of the library are also accessible without VPN
- Here is an [overview](#) of the services for which you need VPN

Lecture transmission (live): For the transmission of lectures we will provide sufficient licenses of the software "Zoom" from the first week of April on. For Zoom we will also add a discussion group to WueCampus. You will also not need a VPN to use Zoom. You can find more information [here](#), a short manual can be found [here](#).

**Documents, screencasts, videos, eLearning:** Of course, our eLearning platform WueCampus is at your disposal. WueCampus has been equipped with additional hardware resources to manage the expected upload of teaching materials. However, we would like to ask for your cooperation: Try to keep the files uploaded to WueCampus small. For media enrichment of content we suggest, for example, the use of audio tracks in PowerPoint, which results in much smaller files compared to video recordings of lectures. (See also the website "[Lehre Digital](#)").

Additional [Camtasia](#) licenses are available in the webshop for creating screencasts. It doesn't take much to create home office videos, a few tips can be found [here](#).

To a limited extent, we have again provided slots for regular lecture recordings for the coming semester. You can reserve a recording in [13 fixed lecture rooms](#). In addition, from the beginning of April, we have equipped some rooms in the central lecture hall and seminar building (Z6) with "recording equipment" for you, where you can obtain instructions and equipment as well as online support if required. More information can be found [here](#), a reservation is possible [here](#).

The "Lecture" service is available for the provision of recordings, videos and screencasts. Due to the expected amount of videos, we will provide another video

streaming server integrated into WueCampus towards the end of April, which will provide additional capacity for the provision of videos.

For reasons of data protection, we would advise against uploading to YouTube as long as the alternatives shown here are available with high performance. The media stored there are basically always freely available worldwide and cannot be restricted for a certain user group!

**Software:** The current measures to contain the corona virus and the associated closure of the University of Würzburg have resulted in some extensions to the software offering on Studisof.de. Details on the expansion can be found in the [list of software products](#).

Even though we have done a lot in the last few weeks to prepare the university for research, teaching and administration in the coming weeks, the technical resources remain very limited. They can make a significant contribution to ensuring that the operation of many processes can be maintained for everyone. I would like to thank you in advance for this.

Yours sincerely,  
Matthias Funken

All information summarized again:

<https://www.rz.uni-wuerzburg.de/aktuelles/mitteilungen/single/news/homeoffice-fuer-forschung-und-lehre-in-zeiten-von-corona/>



## 2. Homeoffice in der Corona-Krise

Teilweise sehr schnell und letztlich für viele überraschend musste seit Mitte März ein Großteil der Arbeit von innerhalb der Universität nach Hause verlegt werden. Hierbei stellen sich diverse Fragen nach Erreichbarkeit per Telefon oder Mail, aber natürlich auch nach der Erreichbarkeit der IT-Dienste und der Nutzbarmachung am dienstlichen oder privaten Notebook zu Hause.

Manches geht nur eingeschränkt, aber die meisten Dienste sind auch von zu Hause aus nutzbar. Die folgende Webseite bietet eine gute Übersicht, welche Voraussetzungen dabei zu beachten sind und welche Tools dabei eine Unterstützung geben können:

<https://www.rz.uni-wuerzburg.de/dienste/arbeitsplaetze/heimarbeit-in-der-coronakrise/>



### 3. Sichere IT-Nutzung im Homeoffice

Mit der gerade geschilderten, plötzlich erforderlichen Heimarbeit darf aber ein anderes wichtiges Thema nicht untergehen: Die IT-Sicherheit - auch und gerade jetzt. Wir möchten Sie an dieser Stelle noch einmal für die grundlegenden Sicherheitsmaßnahmen speziell zu Hause sensibilisieren:

- Generell sollten natürlich auch beim mobilen Arbeiten vergleichbare Sicherheitsvorkehrungen wie beim Arbeiten an der Dienststelle getroffen werden. Diese finden Sie zusammengefasst auch in unseren [goldenen Regeln der Arbeitsplatzsicherheit](#).
- Falls Sie keine Möglichkeit haben, in einem separaten Raum zu arbeiten, achten Sie besonders darauf, Ihren PC beim Verlassen gegen unberechtigten Zugriff zu sperren, z.B. mittels "Windows-Taste + L". Halten Sie zusätzlich während Ihrer Abwesenheit vom Arbeitsplatz nach Möglichkeit Fenster und Türen zum Arbeitsplatz geschlossen.
- Bewahren Sie Ausdrücke und externe Datenträger möglichst sicher, z.B. in einem verschlossenen Rollcontainer oder einer verschlossenen Schublade auf.
- Schließen Sie nach Möglichkeit Fenster und Türen während Sie telefonieren oder an Videokonferenzen teilnehmen um unberechtigten Personen das Mithören zu erschweren.
- Seien Sie besonders aufmerksam bei verdächtigen Mails oder Kontaktaufnahmen angeblicher Kolleginnen und Kollegen über ungewöhnliche und normalerweise nicht genutzte Kanäle und Chat-Tools. Kriminelle versuchen bereits aktiv die Verunsicherung in der Bevölkerung und die neuen ungewohnten Arbeitsbedingungen für ihre Zwecke auszunutzen.
- Stellen Sie unbedingt sicher, dass das verwendete Betriebssystem immer auf dem aktuellsten Stand ist und auch Ihre Anti-Viren-Software aktuell gehalten wird.
- Speichern Sie keine dienstlichen Daten unverschlüsselt auf Ihrem Endgerät. Dies gilt besonders dann, wenn Sie ein privates Endgerät benutzen. Verwenden Sie z.B. VeraCrypt, um einen verschlüsselten Container zu erstellen, in dem Sie für die Zeit des mobilen Arbeitens dienstliche Daten ablegen. Dies hat auch den Vorteil, dass beim späteren Löschen dieses Containers die darin enthaltenen Daten sicher gelöscht werden und von Dritten nicht wiederherstellbar sind. Eine Schritt-für-Schritt Anleitung zum Erstellen eines solchen Containers finden Sie unter <https://go.uniwue.de/veracrypt>
- Bitte denken Sie ebenfalls daran, den Downloadordner Ihres Browsers von dienstlichen Dateien zu bereinigen.
- Benutzen Sie zum Dateiaustausch die von der Universität bereitgestellten Dienste wie z.B. die [Netzlaufwerke \(webbasierter Zugriff\)](#) oder [Teamdrive](#). Tauschen Sie keine dienstlichen Dateien über öffentliche Dienste wie Google Drive, Firefox Send o.ä. aus. Verzichten Sie auch darauf, Dateien in nur temporär genutzte Dienste wie z.B. Microsoft Teams hochzuladen.
- Entsorgen Sie keine dienstlichen Daten in Form von z.B. Ausdrucken oder Datenträgern über ihren Hausmüll ohne diese zuvor unkenntlich gemacht bzw. fachgerecht gelöscht zu haben.
- Nutzen Sie das Universitäts-VPN nur, wenn nötig. Nähere Informationen über das VPN und für welche Dienste es zwingend erforderlich ist finden Sie unter [go.uniwue.de/vpn-corona](https://go.uniwue.de/vpn-corona).
- Beachten Sie bitte auch den Aufruf des CIO der Universität zum "Fair Share" Verhalten unter [go.uniwue.de/fair-share-corona](https://go.uniwue.de/fair-share-corona).
- **Und zu guter Letzt:** Achten Sie auch beim mobilen Arbeiten auf regelmäßige Pausen, sorgen Sie für Ausgleich und bleiben Sie gesund!



#### 4. Digitale Lehre im Sommersemester

Die Frage, die uns aktuell per Mail, Telefon oder Ticketsystem am häufigsten erreicht, lautet: „Wir möchten/müssen die Lehre für das anstehende Sommersemester digital abhalten. Können Sie uns dazu helfen?“

Auch hierzu haben wir auf den Webseiten des Rechenzentrums umfangreiche Informationen zusammengetragen. Grundsätzlich können wir im Augenblick zu den bislang schon bestehenden Diensten (wie z.B. DFNConf oder Adobe Connect des DFN-Vereins) Support leisten, ebenso natürlich für die vom Rechenzentrum direkt angebotenen Dienste wie WueCampus, Lecture, CaseTrain, etc.).

Für die Zeit der in der Krise neu eingeführten Dienste wie z.B. Zoom oder Microsoft Teams bitten wir Sie, zunächst aufmerksam die entsprechenden Hilfeseiten zu studieren und erst dann wegen möglicher Fragen auf uns zuzukommen. Eine intensivere Beratung ist von unserer Seite leider nicht möglich.

Folgende Webseiten bieten eine Übersicht zu den verschiedenen Optionen:

<https://www.rz.uni-wuerzburg.de/aktuelles/mitteilungen/single/news/homeoffice-fuer-forschung-und-lehre-in-zeiten-von-corona/>

und ganz speziell zur digitalen Abbildung der Lehre:

<https://www.rz.uni-wuerzburg.de/dienste/lehre-digital/>



#### 5. Onlineberatung zu IT-Schulungsthemen

Aufgrund der aktuellen Situation wurden natürlich auch die IT-Kurse am Rechenzentrum abgesagt. Aber auch während der Corona-Krise möchten unsere Dozenten Kontakt zu Ihnen halten. Wenn Sie also Fragen rund um die Kursinhalte unserer Präsenzkurse haben, dann melden Sie sich!



**Abbildung 2: Wird es sicher auch wieder geben: Präsenzkurse zu IT-Themen (Foto:RZ)**

Das Schulungsteam Peter Wermke und Winfried Seimert steht Ihnen auch weiterhin hinsichtlich möglicher Fragen für die von ihnen durchgeführten Kurse (siehe dazu die Angebotsübersicht im [KursShop](#))

zur Verfügung.

Schreiben Sie einfach eine Mail an:

[it-support@uni-wuerzburg.de](mailto:it-support@uni-wuerzburg.de)

Die Kollegen werden sich zeitnah mit Ihnen in Verbindung setzen. Sobald der normale Kursbetrieb wiederaufgenommen wird, informieren wir Sie über das aktualisierte Programm. Bitte beachten Sie dazu die Ankündigungen auf der Homepage der Universität und des Rechenzentrums.



## 6. Neue Passwortregeln erfordern Handeln der Benutzer

Der Vorfall mit dem Trojaner „Buran“ im Herbst 2019 war zwar nicht **der** Anlass, aber sicher ein weiterer Motivationsschub, an einer möglichen Stellschraube zur IT-Sicherheit noch etwas zu justieren.

Die Rede ist von der Sicherheit von Passwörtern und wie man diese mittelfristig erhöhen kann. Dazu gab es in den vergangenen Monaten zahlreiche Beratungen im Rechenzentrum, um ein höheres Sicherheitslevel zu erreichen.

Was ändert sich also? Ab dem **15.4.2020** gelten neue Passwortregelungen zunächst für **alle neuen Passwörter** und **neuen Benutzerkonten**. Ab **spätestens Januar 2021** müssen auch **alle bestehenden, alten Passwörter** den **neuen Regeln** entsprechen.

**Was Sie dazu tun müssen, zeigt Ihnen die folgende Übersicht:**

<https://www.rz.uni-wuerzburg.de/aktuelles/mitteilungen/single/news/neue-passwortrichtlinien-fuer-universitaere-benutzerkonten-ab-dem-1542020/>



## 7. Was tun bei Phishing-Mails?

So ziemlich jeder, der ein Mail-Postfach hat, hat sie schon vorgefunden: Mails meist unbekanntem Ursprungs mit teils merkwürdigen Aufforderungen, z.B. seine Kontodaten Preis zu geben oder sein Mailkonto zu überprüfen, weil angeblich keine Mails mehr ausgeliefert werden können.

Mittlerweile verfeinern aber die Hacker ihre Methoden. Es sind schon Fälle vorgekommen, wo durch Absenderfälschung von Mails vermeintlich authentische Anfragen eingetroffen sind und man weniger argwöhnisch ist, als bei gänzlich unbekanntem Kontakten. Oder man erhält - wie im Herbst letzten Jahres geschehen - eine Nachricht, dass ein sogenanntes „eFax“ eingegangen ist. Auch hier kann durch zu schnelle Klicks auf die darin enthaltenen Verlinkungen viel Unheil entstehen.

Beachten Sie daher **folgende Grundregeln** im Umgang mit Mails allgemein:

- Führen Sie grundsätzlich keine Software aus, die Ihnen als E-Mail-Anhang zugesandt wird.
- Deaktivieren Sie im E-Mail-Programm die automatische Anzeige bzw. das Ausführen von E-Mail-Anhängen.
- Misstrauen Sie E-Mails, die die Aufforderung enthalten, Software zu installieren oder Passwörter, Kreditkartennummern, PINs, TANs oder ähnliches zu übermitteln.
- Antworten Sie nicht auf E-Mails mit unerwünschtem oder zweifelhaftem Inhalt, auch nicht, um die Versendung dieser E-Mails abzubestellen.
- Virenbefallene E-Mails täuschen in der Regel vertraute Absenderadressen vor. Misstrauen Sie unerwarteten E-Mails und insbesondere ihren Dateianhängen.
- Deaktivieren Sie nach Möglichkeit die HTML-Ansicht von E-Mails und nutzen Sie stattdessen die Textansicht.
- Prüfen sie alle auf den Rechner geladenen Dateien mit einem Virens scanner.



## 8. Neuer FTP-Server in Betrieb genommen

Viele FTP-Server, vor allem aber die an Universitäten und Fachhochschulen bieten sogenanntes „Anonymous FTP“ an. Solche FTP-Server werden auch als „Pub“ (von engl. Public, „öffentlich“) bezeichnet. Der Zugriff ist also öffentlich und normalerweise über ein bekanntes Passwort oder ganz ohne einer PW-Eingabe möglich.

Auch das Rechenzentrum der JMU betreibt seit langer Zeit einen Anonymous-FTP-Server und hat diesen nun grundlegend neu aufgebaut sowie die gespiegelten Seiteninhalte anderen FTP-Server entsprechend aktualisiert.

Weitere Informationen zu diesem Service finden Sie auf den [Webseiten des Rechenzentrums](#), der direkte Zugang ist hier möglich:

<ftp://ftp.rz.uni-wuerzburg.de/>



## 9. Der IT-Support fragt nie nach Passwörtern!

Ende der Nachricht... ;-) )



Ende des Newsletters April 2020