



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

LEITFADEN

Informationssicherheit – Sicheres Handeln im
Hochschulalltag für Studierende



Inhalt

Vorwort.....	3
Passwortdiebstahl	3
Sicheres Passwort – Gewusst wie.....	5
E-Mails	5
Mobilgeräte und Datenträger	5
Erkennen von Phishing Mails.....	7
Mitschnitte von Vorlesungen	8
Eduroam	8
Cloudspeicher	8
Nutzung von Office365.....	8
Shibboleth – Single-Sign-On	9
Schlussappell	9
Kontakte und Notrufnummern	9

Vorwort

Die Studierenden sollten die Bedeutung von Informationen für den Erfolg der Hochschule kennen: In der Regel elektronisch erstellt, verarbeitet und gespeichert, sind sie seit jeher Grundlage unseres Alltags und stellen eigenständige Hochschulwerte dar. Informations- und Kommunikationstechnik ist heute ein fester Bestandteil der wichtigsten Hochschulprozesse. Ein wirkungsvoller Schutzschild erfordert neben angemessenen technischen Sicherheitsmaßnahmen und Notfallplänen ein Mitwirken der Studierenden.

Genau hier setzt dieser Leitfaden an. Er soll Sie als Studierende anhand von Praxisbeispielen auf konkrete Risiken und Gefahren in ihrem Studienalltag aufmerksam machen, einen kompakten und allgemein verständlichen Überblick über das Thema Informationssicherheit geben und zu Eigenverantwortung motivieren. Konkrete Verhaltensregeln am Ende jedes Kapitels unterstützen Sie bei der Umsetzung des Gelernten und ermöglichen zugleich eine Analyse der eigenen Situation.

Passwortdiebstahl

Hintergrund und Risiken

Die Arbeit am PC beginnt mit der Eingabe eines Passworts. Das soll den PC und das Netzwerk der HWR Berlin vor unbefugtem Zugang schützen. Auch Ihr E-Mail-Konto und andere Accounts werden durch Passwörter gesichert. Leider sind Menschen im Umgang mit ihren Passwörtern oft weniger vorsichtig als mit ihrem Haustürschlüssel, obwohl beide doch einem ähnlichen Zweck dienen.

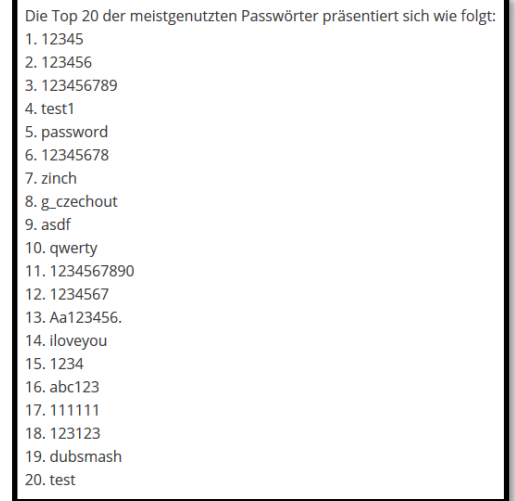
Ausspionieren von Passwörtern

Würden Sie mit einer dieser Kombination Ihre Wohnung schützen? Mit Sicherheit nicht. Gerät ein Passwort in falsche Hände, kann das für Sie und für die HWR Berlin einen großen Schaden zur Folge haben (z. B. Datendiebstahl, Spam-Versand über Ihren E-Mail-Account, Blacklisting Ihrer bzw. der HWR-Emailadressen nach einem Spamversand von einer Studierendenmailadresse, aber auch Interneteinkäufe in Ihrem Namen).

Die Wahl unseres Passworts bietet eine Angriffsfläche für Missbrauch. Besteht eine direkte Verbindung zum Studierenden, zum Beispiel indem das eigene Geburtsdatum oder die Namen der Kinder, des Ehepartners oder

des Haustiers verwendet werden, haben Personen, die sich in Ihrem näheren Umfeld befinden oder sich anderweitig Zugriff zu diesen Informationen beschaffen können, dadurch ein leichtes Spiel. Denken Sie immer an Social Media.

Mit eigentlich sicheren Passwörtern wiederum wird es Angreifern nicht selten durch unbedachtes „Verstecken“ von Passwortzetteln unter der Tastatur oder am Bildschirmrand besonders leichtgemacht.

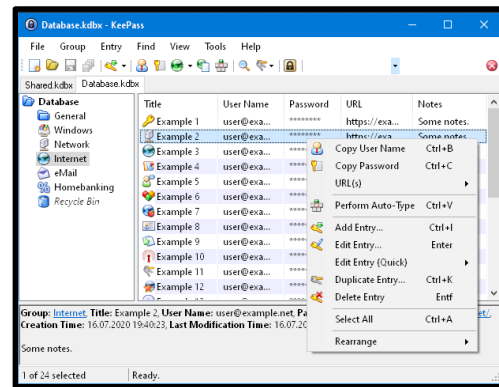


Die Top 20 der meistgenutzten Passwörter präsentiert sich wie folgt:

1.	12345
2.	123456
3.	123456789
4.	test1
5.	password
6.	12345678
7.	zinch
8.	g_czechout
9.	asdf
10.	qwerty
11.	1234567890
12.	1234567
13.	Aa123456.
14.	iloveyou
15.	1234
16.	abc123
17.	111111
18.	123123
19.	dubsmash
20.	test

Passwortmanager

Ein Passwort-Manager, auch Kennwort- oder Passwortverwaltung (englisch Password Manager, Password Safe) genannt, ist eine Anwendungssoftware, mit deren Hilfe ein Nutzer Zugangsdaten verschlüsselt speichern, verwalten und verwenden kann. Die IT der HWR Berlin verwendet und empfiehlt das Programm KeePass.



Brute-Force-Angriff

Bei einem Brute-Force-Angriff werden durch einen leistungsstarken Computer automatisiert alle möglichen Zeichenkombinationen für ein Passwort ausprobiert. Heutzutage prüft ein durchschnittlicher Computer gut mehrere Millionen Passwörter pro Sekunde. Bei einem Passwort, das nur aus einer reinen Zahlen- oder Buchstabenkombination besteht, ist eine solche Suche schnell erfolgreich.

Wörterbuchangriff

In Wörterbuch-Attacken werden durch spezielle Programme mithilfe von umfangreichen Passwortlisten (auch Wordlists oder Dictionaries) typische Wörter und Wortkombinationen (auch aus Fremdsprachen) nacheinander getestet. Dies erfordert weniger Versuche als Brute-Force-Angriffe.

Passwortänderung

Sollten Sie den Verdacht hegen, dass Ihr Passwort nicht mehr geheim ist ändern Sie dieses umgehend!

Verhaltensregeln

- Starke Passwörter: Verwenden Sie zur Absicherung Ihrer Daten nur komplexe Passwörter. Ein sicheres Passwort
 - hat eine angemessene Länge von 8 Stellen, besser 10 bis 15 Zeichen – je mehr Zeichen desto besser
 - enthält sowohl Buchstaben (keine Umlaute) als auch Ziffern (0–9)
 - enthält Groß- und Kleinbuchstaben und Sonderzeichen (z. B. #,\$)
 - enthält keine personenbezogenen Daten (z. B. Name des Haustiers)
 - ist in keinem deutschen oder Fremdwörterbuch enthalten
 - wird in regelmäßigen Abständen (z. B. alle 12 Monate) geändert. Verwenden Sie bei der Erstellung neuer Passwörter keine bereits einmal genutzten Passwörter.
 - Ändern Sie einmal benutzte Passwörter nicht nur geringfügig ab, sondern erstellen diese komplett neu.
- Diskretion: Geben Sie Ihr Passwort niemals an Dritte.
- Aufbewahrung: Behalten Sie Ihre Passwörter am besten im Kopf oder nutzen Sie einen Passwortmanager.
- Eingabe: Achten Sie bei der Passwordeingabe darauf, dass niemand Sie beobachtet. Warten Sie mit der Passwordeingabe, bis Sie unbeobachtet sind.

Sicheres Passwort – Gewusst wie

So merken Sie sich Ihr Passwort leicht!

Starke Passwörter entstehen durch außergewöhnliche Zeichenkombinationen, müssen aber nicht unbedingt kompliziert sein, wie Sie an den folgenden Methoden und Beispielen sehen können:

Akronymmethode

Denken Sie sich einen Satz aus und benutzen Sie von jedem Wort nur den 1. Buchstaben (oder nur den 2., den letzten etc.). Anschließend werden bestimmte Buchstaben in Zahlen oder Sonderzeichen verwandelt.

Beispiel: I want to be called the Number 1 > lwtbct#1

Mehrwortmethode

Überlegen Sie sich mindestens zwei Wörter und verbinden Sie die ersten Buchstaben jedes Wortes miteinander ohne ein Leerzeichen dazwischen.

Beispiel: HerrMüllerundFrauSchneider > HMue#FSc

E-Mails

Hintergrund und Risiken

E-Mails erleichtern die Kommunikation und den Informationsaustausch in der Hochschule und tragen zu einem effizienteren Arbeitsablauf bei. Doch wussten Sie, dass die HWR Berlin nach Ihrer Immatrikulation ausschließlich Ihre von der IT bereitgestellte Studierendenmailadresse zur Kommunikation nutzen darf?

Verhaltensregeln

- Nutzen Sie für die Kommunikation mit Professoren oder Mitarbeitenden der HWR Berlin ausschließlich ihren, von der HWR Berlin bereitgestellten, E-Mail-Account.
- Prüfen Sie Ihren Postausgang regelmäßig, um sich zu vergewissern, dass von Ihrem Account keine Spammails versandt werden.
- Melden Sie Spamversand aus Ihrem Postfach umgehend der IT der HWR.

Mobilgeräte und Datenträger

Hintergrund und Risiken

Es entstehen beim Verlust von Laptops, Mobilfunkgeräten und mobilen Datenträgern (Festplatten, USB-Sticks) nicht nur Kosten für die Wiederbeschaffung, sondern es droht auch Vertraulichkeits- oder Datenverlust, wenn dadurch fremde Personen unbefugten Zugriff auf hochschulinterne Informationen, Ihre persönlichen Daten oder personenbezogene Daten anderer erhalten.

Bitte gehen Sie deshalb mit Ihren Mobilgeräten und Datenträgern besonders sorgsam um!

Gelegenheit macht Diebe

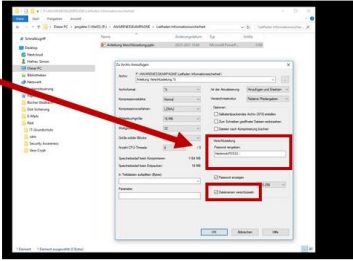
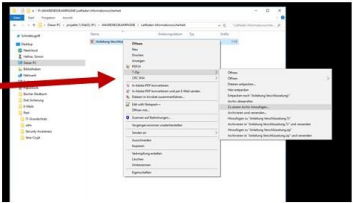
Geben Sie Dieben keine Chance und bewahren Sie Ihr Gerät unterwegs so sicher und unauffällig wie möglich auf. Transportieren Sie das Gerät auf Zug- oder Flugreisen im Handgepäck und auf Autofahrten von außen unsichtbar im Kofferraum.

Verschlüsselung der Daten

Vertrauliche Daten sollten verschlüsselt werden. So wird sichergestellt, dass bei Verlust des Notebooks oder mobilen Datenträgers nur ein materieller Schaden entsteht – die darauf gespeicherten Daten können nicht ausgespäht werden. Eine einfache Anleitung für Dateiverschlüsselung finden Sie für das kostenlose Tool 7-Zip im Bild unten.

Anleitung zum Verschlüsseln von Dateien

1. Datei auswählen und Rechtsklick
2. „7-Zip“ auswählen
3. „Zu einem Archiv hinzufügen“ auswählen
4. Passwort eingeben
5. Haken setzen bei „Dateinamen verschlüsseln“
6. OK betätigen



Fremde Datenträger abgeben

Sollten Sie in der HWR Berlin einen fremden Datenträger, zum Beispiel einen USB-Stick oder eine Speicherkarte, finden, geben Sie ihn direkt beim IT-Helpdesk ab. Schließen Sie einen fremden Datenträger niemals an Ihrem Computer an, es könnten Schadprogramme auf Ihrem Computer installiert werden.

Achten Sie auf Ihre Datenträger

Passen Sie gut auf Ihre eigenen Datenträger und Geräte auf, denn bei Verlust oder Diebstahl könnten vertrauliche Daten an Dritte gelangen. Achten Sie zudem auf eine möglichst sichere Verwahrung. Speichern Sie Daten von mobilen Datenträgern regelmäßig auf einem Backuplaufwerk. Wenn Sie einen Datenträger außer Betrieb nehmen, sollte sichergestellt sein, dass alle darauf gespeicherten Daten gelöscht bzw. unbrauchbar gemacht sind.

Verhaltensregeln

- Verschlüsselung: Speichern Sie keine vertraulichen Daten unverschlüsselt auf mobilen Datenträgern.
- Zugangsschutz: Schützen Sie Ihre mobilen IT-Geräte vor Zugriff von Dritten. Sperren Sie Ihr Gerät mittels eines Passwortes oder PIN-Codes und sperren Sie den Bildschirm bei Inaktivität
- Datenübertragung: Lassen Sie nur kontrollierte Datenübertragungen zu. Schalten Sie insbesondere die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur dann ein, wenn Sie diese bewusst zur Kommunikation mit bekannten Geräten und Netzen nutzen.
- Fremde Datenträger: Geben Sie fremde Datenträger beim IT-Helpdesk ab und schließen Sie sie niemals an Ihrem Computer an!
- Entsorgung: Sorgen Sie bei Außerbetriebnahme bzw. Vernichtung eines Mobilgerätes oder Datenträgers dafür, dass alle darauf gespeicherten Daten sicher gelöscht bzw. unbrauchbar sind.

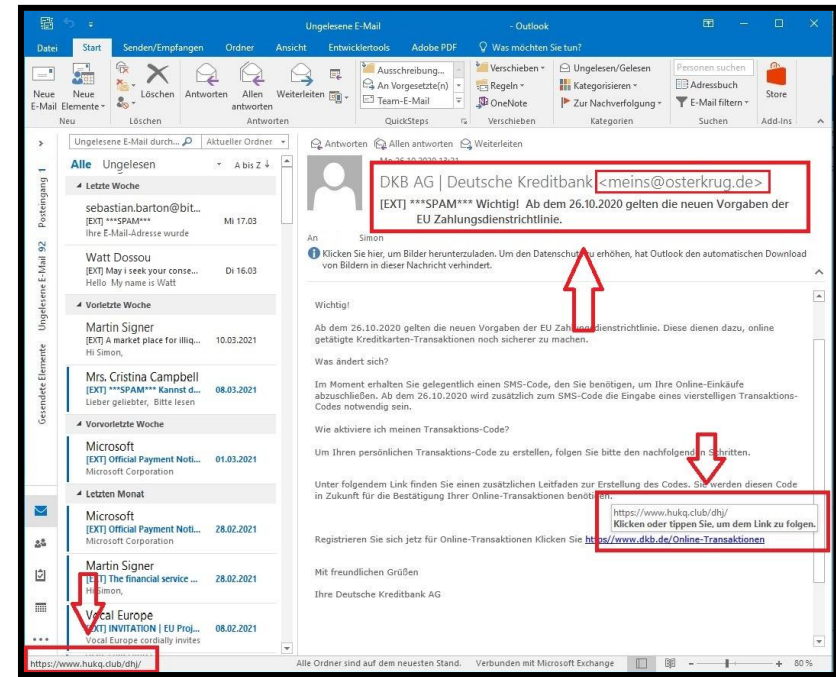
Erkennen von Phishing Mails

Hintergrund und Risiken

Das beliebteste Mittel, um an Ihre Daten zu gelangen, ist die klassische Phishing Mail. Dabei versuchen Betrüger verschiedene Verhaltensweise der Nutzer auszunutzen. Phishing Mails können Druck auf Sie ausüben, könnten Ihnen zu Themen, die Sie interessieren vermeintlich interessante Informationen liefern, Sie könnten nach Hilfe gefragt werden oder Betrüger könnten darauf hoffen, dass Sie schlicht unaufmerksam sind. Daher ist es wichtig eingehende Mails auf Plausibilität zu prüfen, bevor mit diesen interagiert wird. Gibt der Inhalt vor von Amazon zu stammen, die E-Mail-Adresse des Absenders hat jedoch keinen Bezug zu Amazon, oder Sie sind überhaupt nicht Kunde von Amazon, dann liegt hier höchstwahrscheinlich ein Phishingversuch vor.

Selbst wenn in der E-Mail ein Link zu <https://www.amazon.de/> zu finden ist, kann dieser zu einer anderen Seite führen, wie bei diesem Link auch.

Probieren Sie es aus! Daher ist es wichtig, die Zieladresse zu ermitteln, bevor Sie auf den Link klicken. Dies machen Sie einfach indem Sie mit der Maus über den Link wandern. In der Regel wird Ihnen dann in einem Pop-Up die wahre Adresse angezeigt. Sollte kein Pop-Up aufgehen, dann steht der Link unten in der Statusleiste. Ebenso senden Betrüger gerne Mailanhänge mit schadhaftem Inhalt. Daher ist es hier auch wichtig die Dateiendung zu prüfen, bevor Mailanhänge geöffnet werden. Haben Sie keinen Mailanhang vom Gesprächspartner angefordert? Dann öffnen Sie diesen auch nicht! Fragen Sie notfalls beim Gesprächspartner nach, nutzen Sie dafür aber niemals die Kontaktdaten aus der E-Mail, sondern greifen auf Suchmaschinen oder bereits bekannte Kontaktinformationen zurück. Ausführliche Hinweise zum Erkennen von Phishing Mails entnehmen Sie dem Flyer zu Phishing Mails.



Verhaltensregeln

- Prüfen Sie ob Absenderadresse und Inhalt zusammenpassen.
- Ermitteln Sie die Zieladresse möglicher Links in der Mail ohne zu klicken.
- Identifizieren Sie die Domain in der Zieladresse.
- Prüfen Sie ob die Domain auch zum Absender passt.
- Kennen Sie die Domain nicht, nutzen Sie eine Suchmaschine um Informationen zur Domain zu erhalten.
- Schauen Sie sich die Dateiendungen möglicher Anhänge an, ohne diese anzuklicken.
- Klicken Sie potentiell gefährliche Dateien wie .exe, .docm, etc. nur an, wenn Sie diese genau in diesem Format vom Absender gefordert haben.

Mitschnitte von Vorlesungen

Das Aufzeichnen von Vorlesungen ist aus Datenschutzgründen für Studierende leider grundsätzlich nicht erlaubt. Weder im Präsenzbetrieb noch im Fernunterricht dürfen Vorlesungen aufgezeichnet werden. Dies gilt sowohl für die Video-, als auch für die Audiomitschnitte. Bei der Aufzeichnung von Vorlesungen sind sowohl das Urheberrecht wie auch das Recht auf informationelle Selbstbestimmung betroffen. Nur mit einer ausdrücklichen Einwilligung des Lehrenden können Mitschnitte angefertigt werden - **dies gilt im Übrigen auch für Aufzeichnungen der Lehrenden.**

Eduroam

Ihnen steht Eduroam an allen Europäischen Hochschulen zur Verfügung. D.h. Sie können sich an allen teilnehmenden Institutionen mit Ihrem HWR-Eduroam-Login ins WLAN einwählen. Eduroam darf jedoch ausschließlich in einem rechtskonformen Weg verwendet werden. D.h. dass Eduroam nur für legale Zwecke genutzt werden darf. Dazu zählen nicht: Musik- oder Filmdownloads, Hackingaktivitäten oder andere Handlungen mit strafrechtlich relevantem Bezug.

Cloudspeicher

Nutzen Sie für Dokumente, die Sie im Rahmen ihres Studiums mit anderen Studierenden teilen möchten, den von der HWR Berlin angebotenen persönlichen und kostenlosen [Cloudspeicherplatz](#). Dieses Angebot wurde datenschutzrechtlich geprüft. Die Datenverarbeitung erfolgt hierbei ausschließlich innerhalb der HWR Berlin. Somit werden Ihre Daten nicht an Datenkraken wie Microsoft, Dropbox oder Google übermittelt.

Andere (meist kostenlose) Clouddienstleister sind unter Studierenden beliebt und in ihrem Studienalltag möglicherweise schon im Einsatz. In diesen Geschäftsmodellen fällt es meist schwer nachzuvollziehen, wo Ihre Daten lagern und wie der Anbieter die Daten verarbeitet bzw. nutzt. Oft behalten diese sich vor, die hochgeladenen Dateien für eigene Zwecke zu nutzen z.B. zur Bildung von Nutzerprofilen, Gesichtserkennung oder anderen Mustererkennungen.

Jeder Studierende kann sich hier an der HWR-Cloud anmelden:

<https://cloud.hwr-berlin.de>

Nutzung von Office365

Die HWR Berlin stellt den Studierenden eine kostenlose Lizenz für Microsoft Office365 zur Verfügung. Es handelt sich um ein Paket an nützlichen Cloudanwendungen für den Studierendenalltag. Die Nutzung ist in jedem Fall freiwillig und findet auf eigene Verantwortung statt. D.h. die HWR Berlin übernimmt keine datenschutzrechtliche Verantwortlichkeit im Zuge der Nutzung durch die Studierenden.

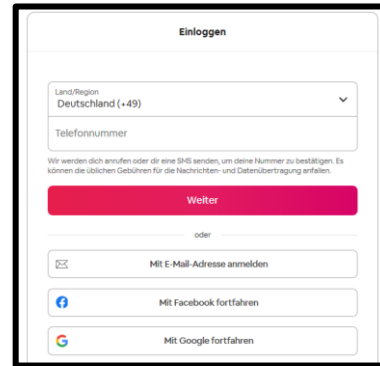
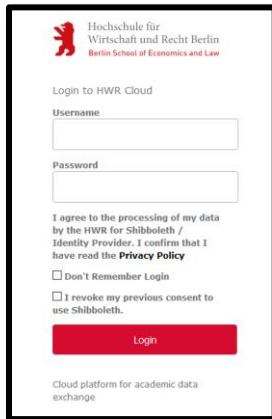
Shibboleth – Single-Sign-On

Single-Sign-On (auch „Einmalanmeldung“) dürfte vielen bereits ein Begriff sein ohne genau zu wissen, worum es sich handelt. Facebook, Google und Co.

Bieten oft die Möglichkeit, dass der Nutzer sich unkompliziert mit den Google Zugangsdaten auch auf anderen Seiten anmelden kann. Ziel des Single Sign-on ist es, dass sich der Benutzer nur einmal unter Zuhilfenahme eines einzigen Authentifizierungsverfahrens (z. B. durch Passwortheingabe) identifizieren muss. Das

hat den Vorteil, dass sich der Nutzer nur ein Passwort merken muss, welches dafür umso sicherer sein muss. Bei Verlust oder Kompromittierung des Passworts sind alle Dienste betroffen.

Die HWR Berlin nutzt Shibboleth als Single-Sign-On-Dienst. Derzeit sind nur einige wenige interne Dienste angebunden wie z.B. die HWR-Cloud. Das Angebot an angebundenen Diensten wird jedoch sukzessive ausgebaut werden.



Schlussappell

Bleiben Sie wachsam!

Handeln Sie bedacht und befolgen die Hinweise in diesem Leitfaden um unbeschwert durchs Studium zu kommen. Bei Fragen stehen Ihnen die Ansprechpartner der HWR Berlin gerne zur Verfügung.

Kontakte und Notrufnummern

IT-Helpdesk

it-hotline@hwr-berlin.de / it.hwr-berlin.de / (0)30 30877-2525

IT-Sicherheit

it-sicherheit@hwr-berlin.de / sicherheit.hwr-berlin.de

Datenschutzteam

datenschutz@hwr-berlin.de / datenschutz.hwr-berlin.de