BENUTZERZUGANG

Ihre Passwörter müssen sicher sein!

- Wählen Sie ungewöhnliche Passwörter die nicht erraten werden können und wechseln Sie diese regelmäßig
- Schreiben Sie Ihre Passwörter nicht auf. Jeder böse Mensch schaut zunächst unter Ihrer Tastatur oder in Ihrem Schreibtisch nach.
- Geben Sie Ihre Passwörter niemals weiter! Egal wie gut das Argument Ihres gegenüber ist oder wie bequem Ihnen dieser Vorgang erscheint.
- Nutzen Sie verschiedene Passwörter und nie die selben für formelle und informelle Zugänge.
- Verwenden Sie nach Möglichkeit einen Passwort-Container für eine zentrale und sichere Verwaltung.

➡ An der Hochschule OWL ändern Sie Ihr Passwort über die Benutzerverwaltung.
https://www.hs-owl.de/IDM

- **Benutzerzugang**
- Bildschirmsperre
- Datensicherheit
- Umsicht im Internet
- Social Networking
- Kooperation

BILDSCHIRMSPERRE

Bildschirm sperren am Arbeitsplatz!

- Geben Sie Fremden, aber auch Bekannten niemals die Möglichkeit, Ihren Rechner und somit auch das Hochschulnetzwerk unbefugt zu verwenden.
- Sperren Sie aus diesem Grund immer den Rechner, wenn Sie Ihren Arbeitsplatz verlassen.

➡ Strg + Alt + Entf

- Versehen Sie Ihren Bildschirmschoner bei einer Deaktivierung mit einem Passwortschutz.
- Vermeiden Sie eine automatische Anmeldung beim Start Ihres Rechners.

- Benutzerzugang
- **Bildschirmsperre**
- Datensicherheit
- Umsicht im Internet
- Social Networking
- Kooperation

DATENSICHERHEIT

Sicheres Versenden von Dateien!

Datenübertragung

- Daten sind im Internet ungeschützt. Versenden Sie niemals vertrauenswürdige Unterlagen ohne eine vorherige Verschlüsselung oder andere Sicherheitsmaßnahmen.
- Haben Sie keine Wahl, verwenden Sie wenigstens ein geschütztes ZIP-Archiv und teilen Sie dem Empfänger das dazugehörige Passwort über einen alternativen Kanal mit.
- Ein alternativer Kanal kann bspw. Ihr Telefon oder eine weitere E-Mail sein.

Anmeldung & Dateneingabe

- Achten Sie auf Anmelde- oder Formularseiten stets auf eine gesicherte Verbindung (https). Andernfalls werden Ihre Daten ungeschützt, für dritte mitlesbar, übertragen.
- Gesicherte https-Seiten erkennen Sie im Webbrowser in der URL-Eingabezeile an einem Schloss-Icon

- Benutzerzugang
- Bildschirmsperre
- **Datensicherheit**
- Umsicht im Internet
- Social Networking
- Kooperation

UMSICHT IM INTERNET

Der richtige Weg beim Klicken!

Prüfen Sie Inhalte erhaltener E-Mails auf dienstliche Plausibilität und Vertrauenswürdigkeit. Dies gilt vor allem bei der Aufforderung zur Eingabe von persönlichen Daten oder aber vor dem Öffnen von Anhängen.

Gängige Angriffsmethoden zielen auf 1hr unbedachtes Handeln ab:

➡ **Phishing:**
Falsche Verweise zur Anmeldeseite (Banken, Kreditkarten, Online-Shops)

➡ **Viren:**
Gefährliche Anhänge versenden/manipulieren häufig unbemerkt Ihre Daten.

- Benutzerzugang
- Bildschirmsperre
- Datensicherheit
- **Umsicht im Internet**
- Social Networking
- Kooperation

SOCIAL NETWORKING

Kennen Sie wirklich alle Ihre Freunde?

Seien Sie misstrauisch in sozialen Netzwerken, falsche Freunde versuchen Ihr Vertrauen zu gewinnen um an Ihre persönlichen Daten zu gelangen:

- Haben Sie plötzlich neue Freunde, die sich ausführlich für Ihre Arbeit interessieren?
- Kennen Sie wirklich alle Ihre Freunde in sozialen Netzwerken wie zum Beispiel Facebook oder XING?
- Achten Sie stets darauf, auch im privaten informellen Bereich keine arbeitsspezifischen, vielleicht sogar sensiblen Informationen preiszugeben.

Benutzerzugang
Bildschirmsperre
Datensicherheit
Umsicht im Internet
Social Networking
Kooperation

KOOPERATION

Unterstützen Sie stets aktiv die IT-Abteilung!

Sollten Sie ungewöhnliche Dinge beobachten, die Sie sich nicht erklären können, wenden Sie sich umgehend an Ihren IT-Administrator.

- Anders reagierende Programme
- Veränderungen an Hard- oder Software
- Merkwürdige (nervende) E-Mails

➡ Die Nutzerberatung des S(kim) als persönliche Anlaufstelle

- An den Standorten Lemgo, Detmold und Höxter
- Sowie dem Studienort Warburg
- Hotline: +49 (0) 52 61/702 2222
- E-Mail: support@hs-owl.de
- WWW: hs-owl.de/skim/kontakt
- Hilfe: hs-owl.de/skim/dokumentation

Benutzerzugang
Bildschirmsperre
Datensicherheit
Umsicht im Internet
Social Networking
Kooperation

FAZIT

Ausblick und weitere Tipps

Ausblick

100% Sicherheit wird realistisch wohl nicht zu erreichen sein. Selbst durch größtmöglichen Aufwand im technischen und sozialen Bereich werden Lücken oder besser Gefahren bleiben. Final sind Sie an dieser Stelle als die wohl bedeutendste „Firewall“ gefragt:

➡ „Behalten Sie gerade im Alltag an der Hochschule immer ein gesundes Misstrauen und halten Sie sich stets an die sechs fundamentalen Regeln!“

Weitere Tipps für Ihre digitalen Endgeräte:

- Deinstallieren Sie, wenn noch vorhanden, MS Windows XP und installieren Sie Microsoft Windows 7 oder höher. Gerade bei alten Betriebssystemversionen werden wichtige Sicherheitsaktualisierungen abgekündigt, so dass sie ein höheres Potenzial an Anfälligkeit bieten.
- Verwenden Sie immer einen aktuellen Virenscanner, der so eingeschaltet ist, das er mehrmals am Tag automatische Updates oder neue Signaturen einspielt.
- Achten Sie auf die Aktualität, Ihrer verwendeten Software, da gerade ältere Versionen bekannte Sicherheitslücken enthalten.

0002

SICHERHEIT IN DER IT

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Sicherheitsregeln für die IT

- Benutzerzugang
- Bildschirmsperre
- Datensicherheit
- Umsicht im Internet
- Social Networking
- Kooperation