10 Punkte im Umgang mit sensiblen Daten

Lehrpersonen arbeiten oft mit sensiblen Daten (Informationen zu Schülern, Bilder von Schülern, etc. Um zu verhindern, dass sensible Daten unkontrolliert in der Cloud zu finden sind, ermöglicht die Sekundarstufe Uster den Lehrpersonen einen externen Zugang zu den Daten der einzelnen Schulhäuser. Ausserdem haben die Lehrpersonen externen Zugriff auf die Schul- und Notenverwaltung Lehreroffice.
Um einem Missbrauch dieser Daten vorzubeugen, gilt es folgende Punkte zu berücksichtigen:

1. **Betriebssystem des Computers regelmässig updaten**
2. **Computer mit Antivirensoftware sichern**
3. **Daten mit einer Firewall schützen**
4. **Accounts mit einem komplexen Passwort sichern**
5. **Keine Passwörter weitergeben**
6. **Passwörter nicht aufschreiben**
7. **Keine sensiblen Daten in der Cloud speichern**
8. **Sensible Daten verschlüsseln**
9. **Computer sperren beim Verlassen des Arbeitsplatzes**
10. **Vorsicht bei unbekannten Mails und Anhängen**

1. Betriebssystem des Computers regelmässig updaten

Betriebssysteme und Anwendungen weisen immer wieder Schwachstellen auf, welche die Sicherheit des Computers gefährden. Installiere regelmässig die "Sicherheits-Updates", "Patches" und "Service Packs" der Hersteller, um Schwachstellen zu beseitigen.

2. Computer mit Antivirensoftware sichern

Ein aktueller Virenscanner gehört zum Basisschutz eines jeden Computers. Achte darauf, dass dieser aktiviert ist und auf dem aktuellen Stand gehalten wird.

3. Daten mit einer Firewall schützen

Eine Firewall schützt deinen Computer vor unberechtigten Zugriffen aus dem Internet. Aktuelle Betriebssysteme (Windows, Linux, Mac OS X) bieten dir bereits eine integrierte Firewall für einen Basisschutz an.

4. Accounts mit einem komplexen Passwort sichern

Einfache und kurze Passworte sind leicht zu merken. Aber sie sind nicht sicher.
Für eine ausreichende Passwortsicherheit beachte bitte die folgenden Punkte:

Benutze mindestens acht Zeichen mit Ziffern, Buchstaben und/oder Sonderzeichen.
Verwende keine Passwörter wie Namen, Geburtstage oder Wörter, die in Wörterbüchern stehen.
Benutze unterschiedliche Passwörter.

5. Keine Passwörter weitergeben

Behandle dein Passwort wie die PIN deiner Bankkarte. Gib es nicht weiter, auch nicht wenn du dazu aufgefordert wirst. Von Seiten der Schule werden dich nie nach deinem Passwort fragen.

6. Passwörter nicht aufschreiben

Notiere dir niemals das Passwort. Wenn du Passwörter aufschreiben willst, nutze einen Passwortsafe (Das ist ein Programm, das deine Passwörter sicher aufbewahrt). Oder du merkst dir einen Satz und nimmst davon die Anfangsbuchstaben.
Beispiel:
Seit 5 Jahren arbeite ich an der Sek Uster als Lehrer. → S5JaiadSUaL.

7. Keine sensiblen Daten in der Cloud speichern

Onlinespeicher gelten nicht als sichere Speicherorte, daher ist es auch kein Speicherort für sensible Daten von Schülern.

8. Sensible Daten verschlüsseln

Sichere deine vertraulichen Daten durch Verschlüsselung. Es gibt einfache Gratisprogramme, die du dafür einsetzen kannst. Vergiss aber nicht das Passwort für verschlüsselte Daten. Geht dieses verloren, gehen auch die Daten verloren.

9. Computer sperren beim Verlassen des Arbeitsplatzes

Wenn du deinen Arbeitsplatz verlässt, ist dein Computer nicht geschützt. Jemand kann sich so leicht Zugriff zum Computer verschaffen.

10. Vorsicht bei unbekannten Mails und Anhängen

Eine große Anzahl von "Malware" (schädliche Software wie Viren, Würmer oder Trojaner) werden via Mails verteilt. Öffne daher keine Anhänge von Leuten oder Firmen, die dir verdächtig erscheinen.