



Arbeitsblatt vom

Name:

Sicheres ICQ – weißt du wie? (Teil 1)

! ICQ (vom englischen „I seek you“) ist wohl das bekannteste Programm so genannter „Messenger“. Mit einem Messenger siehst du sofort, wer von deinen Freunden online ist und du kannst Kontakt zu ihnen aufnehmen. Aber ... beim Instant-Messaging (so der Fachausdruck) lauern auch Gefahren, denn ...

Erwachsene, die Kinder belästigen oder ihnen Gewalt antun wollen, könnten mit ihnen über diesen Weg in Kontakt treten. Das ist deshalb gefährlich, weil sie dich hier (anders als im Chat) ganz privat ausfragen können.

Je nach dem, wie du den Messenger einstellst, kann jeder deine persönlichen Daten lesen, wenn du z. B. Adresse, Alter, Hobbys usw. eingetragen hast.

1. Arbeitsauftrag:

„Klicksafe.de“ gibt einige Tipps, wie man sich vor solchen Gefahren schützen kann: Fülle die Tabelle aus, indem du erklärst, warum der jeweilige Tipp sinnvoll ist und finde ein Beispiel dazu.

Tipp	Warum?	Beispiel!
Die Sicherheitseinstellungen verschärfen: z. B. keine Nachrichten von Fremden annehmen, Aufnahme in die Kontaktliste nur mit Erlaubnis zulassen, öffentliche Statusanzeige abschalten.		
Die eigene Messenger-Kennung (Benutzername, ICQ-Nummer, Yahoo-ID etc.) nicht leichtfertig an fremde Personen weitergeben (z. B. in öffentlichen Foren oder Chaträumen).		
Nur wirklich gute Freunde in die Kontaktliste aufnehmen und vor allem auch nur diesen erlauben, einen selbst in deren Liste zu setzen (bei einigen Messengern lässt sich dies nämlich nicht rückgängig machen).		
Öffentlich einsehbare Messenger-Profile möglichst sparsam und zurückhaltend ausfüllen (keine Adresse, Telefonnummer, Alter, Bilder und am besten nur einen Spitznamen).		
Niemals Dateien von unbekanntem Personen annehmen, da diese Viren, Trojaner etc. enthalten können.		
Keinesfalls auf einen Link klicken, ohne sich vorher abgesichert zu haben, dass die jeweilige Person diesen auch willentlich geschickt hat.		
Messenger-Software immer auf dem aktuellen Stand halten und regelmäßig updaten, da bekannt gewordene Sicherheitslücken vom Anbieter behoben werden.		