Benutzerkonto bzw. Netzwerkkonto	Wird z. B. in einer Familie nur ein Computer genutzt, soll für jedes Familienmitglied ein Benutzerkonto eingerichtet werden. So kann jeder Benutzer eigene Einstellungen vornehmen und hat einen von anderen Benutzern getrennten Datenspeicherplatz. Bei der Anmeldung muss sich der Benutzer authentifizieren. **Sicherheitstipp**: Verlässt man den Computerarbeitsplatz, soll man sich abmelden.
Biometrische Verfahren	Biometrische Verfahren werden zur Authentifizierung verwendet: Die Identität eines Benutzers wird durch Gesichtserkennung, Fingerabdruck, Augenhintergrund festgestellt. Biometrische Verfahren ersetzen oder ergänzen in manchen Fällen die Authentifizierung durch Passwörter.
Botnet	Infizierte Computer werden ohne Wissen der Eigentümer zu einem Netzwerk (Botnet) zusammengeschlossen. Die Betreiber von Botnets missbrauchen die Computer z.B. für den Versand von Spam- oder Phishing-Mails.
Cloudspeicher	Das Sichern von Backups auf einen Cloudspeicher haben den Vorteil, dass die Daten zusätzlich an einem anderen Ort aufbewahrt werden, denkt man z. B. an einen Brand oder Hochwasser.
Cloud-Computing	Unternehmen setzen beim Speichern und Verarbeiten von Daten auf die Cloud. Dies hat große Vorteile, birgt aber auch Gefahren, da eventuell unbefugte Personen Zugriff auf die Daten erlangen könnten.
Computerviren	Computerviren sind unerwünschte Programme, welche sich in Computerprogramme einschleusen. Durch den Aufruf eines Programms, das ein Virus infiziert hat, wird dieser aktiv und kann sich weiterverbreiten.
Computerwurm	Malware, die sich selbständig über Netze (Internet) verbreitet. Ein Computerwurm nützt sehr oft Sicherheitslücken zum Eindringen in ein System.
Cracker	Cracker (vom englischen crack für „knacken“ oder „[ein]brechen“) umgehen Zugriffsbarrieren von Computersystemen und Rechnernetzen. Cracker tun dies meist aus Profitstreben.
Cross Site Scripting-Angriffe	*Übersetzt*: Webseitenübergreifende Scripting-Angriffe. Infizierte Webseiten nützen Sicherheitslücken aus. *Beispiel: Die Webseite einer Zeitung infiziert durch Werbeanzeigen, die automatisch von Werbeanbietern bezogen werden, die Rechner der Besucher.*
Cybercrime	Computerkriminalität bzw. Internetkriminalität
Cyber-Grooming	Gezieltes Ansprechen von Minderjährigen im Internet mit dem Ziel der Anbahnung sexueller Kontakte.
Cyber-Mobbing	Mobbing mithilfe von elektronischen Medien: Verbreitung von Unwahrheiten bzw. von bloßstellenden Fotos in sozialen Netzwerken.

Cookies	Cookies sind kleine Textdateien, die Informationen über besuchte Webseiten beinhalten und auf dem PC des Benutzers abspeichert sind. Onlineshops wie Amazon verwenden z.B. Cookies, um Benutzer wiederzuerkennen und den Inhalt des Warenkorbs bei einem wiederholten Besuch wiederherzustellen.
Dateierweiterung	Die Dateierweiterung ist der letzte Teil eines Dateinamens und wird mit einem Punkt abgetrennt. Das Betriebssystem erkennt an der Dateierweiterung das Format einer Datei und kann diese mit einem passenden Programm öffnen. *Dateien vom Typ exe, bat, zip, etc. können Malware enthalten. Beachte: Auch Worddateien können mit aktiven Makros Schaden anrichten.*

Ergänze bzw. beantworte folgende Fragen!

Beim Verlassen des Computerarbeitsplatzes soll man sich **abmelden**.

Cross-Site-Scripting Angriffe nützen auf infizierten Webseiten Sicherheitslücken aus.

Welchen Vorteil, neben vielen anderen, hat ein Cloudspeicher?

A: Sichern von **Daten**.

Wie nenn man Personen, die in Computersysteme einbrechen?

A: Cracker

Wie kann man Internetkriminalität auch nennen?

A: Cybercrime

Wie nennt man Mobbing mit Hilfe von elektronischen Medien?

A: Cyber-Mobbing

Wie nennt man das Netzwerk von Computern, die ohne Wissen der Eigentümer zusammengeschlossen werden?

A: Botnet

Welche Gefahr kann Cloudcomputing für Unternehmen mit sich bringen?

A: Unbefugte Personen könnten Zugriff auf Daten bekommen

Woran erkennt man, um welche Datei es sich handelt?

A: Dateierweiterung

Fotografiere den QR-Code und löse das Quiz.

Erreichte Punkte: _____