Cyber Sicherheit

Vor dem Unterricht...

Im nächsten Unterricht werden wir neuen Wortschatz lernen und diesen praktisch im Unterricht anwenden. Dafür sollten Sie sich den neuen Wortschatz auf der anderen Seite ansehen und die neuen Wörter in der unteren Übung benutzen. Falls Sie Fragen zum Wortschatz haben sollten, verwenden Sie bitte ein Wörterbuch. Die Antworten werden im Unterricht korrigiert.

1. Verbinden Sie die Begriffe mit den Definitionen.

a. die Cyber-Sicherheit	1. Schadsoftware, die dazu entwickelt wurde, unbefugten Zugang zu Computern oder Netzwerken zu erlangen oder diese zu beschädigen.
b. der Hacker / die Hackerin	2. Schutz von Computersystemen und Netzwerken vor Diebstahl oder Beschädigung ihrer Hardware
c. der Virus	3. eine geheime Zeichenfolge, die verwendet wird, um den Zugang zu einem Computersystem oder einer Datei zu kontrollieren.
d. die Firewall	4. eine betrügerische Methode, um sensible Informationen wie Passwörter oder Kreditkartendaten zu erhalten, indem man sich als vertrauenswürdige Quelle ausgibt.
e. die Malware	5. ein Verfahren, bei dem Informationen so umgewandelt werden, dass nur autorisierte Parteien sie lesen können.
f. das Passwort	6. ein schädliches Programm, das sich selbst verbreitet und das System eines Computers beschädigen kann.
g. die Phishing-Attacke	7. eine Sicherheitsvorrichtung, die den Datenverkehr zwischen verschiedenen Netzwerken überwacht und kontrolliert
h. die Verschlüsselung	8. der Schutz persönlicher Daten vor unbefugtem Zugriff und Missbrauch.
i. der Datenschutz	9. Eine Person, die in Computersysteme eindringt, um Daten zu stehlen oder zu manipulieren.

2.Ergänzen Sie die unteren Sätze mit dem Wortschatz auf der anderen Seite.

a.Sei vorsichtig, welche Dateien du herunterlädst. Du könntest dir _____ einfangen.

b. Hast du gehört, dass ein _____ in unser System eingedrungen ist ?

c. „Warum kann ich diese Seite nicht öffnen?“ - „Vielleicht blockiert die _____ den Zugang.“

d. „Wie oft änderst du dein _____?“ - „Mindestens einmal im Monat, um sicher zu sein.“

e. Unsere Kommunikation ist sicher, weil wir _____ verwenden.

f. Warum muss ich so viele Zustimmungen geben?“ - „Das dient alles dem _____ deiner persönlichen Daten

g. Mein Computer ist total langsam. Ich glaube, ein _____ hat ihn infiziert.

h. Die zunehmende Bedrohung durch Hacker und Malware unterstreicht die Notwendigkeit einer starken _____ in Unternehmen und Behörden.

i. Ich habe eine E-Mail bekommen, die nach meinen Bankdaten fragt. Könnte das eine _____ sein?

CEFR B2 C1 C2

Cyber Sicherheit

Start

1. Was sind einige der häufigsten Bedrohungen für die Cyber-Sicherheit in unserem Alltag?
2. Warum ist es wichtig, persönliche Daten im Internet zu schützen, und welche Maßnahmen können dazu beitragen?

Wortschatz

der Hacker / die Hackerin
der Virus
die Firewall
die Malware
das Passwort

die Verschlüsselung
der Datenschutz
die Cyberattacke

die Phishing-Attacke
der Trojaner
die Sicherheitslücke
der Diebstahl
der Datenverkehr

infizieren / blockieren /aktualisieren/ beschädigen /stehlen

Schlüsselsätze

Sehen wir uns die Schlüsselsätze an, welche Ihnen beim Sprechen helfen werden.

Cyber-Sicherheit ist heutzutage ein wichtiges Thema, das uns alle betrifft.
In einer zunehmend digitalisierten Welt ist der Schutz unserer Daten und Systeme von entscheidender Bedeutung.
Ich bin der Meinung, dass Unternehmen mehr in die Schulung ihrer Mitarbeiter investieren sollten, um die Sicherheitsbewusstsein zu stärken.
Es gibt verschiedene Arten von Malware wie Viren, Würmer und Trojaner, die unsere Systeme gefährden können.

Die Implementierung von Firewalls und Verschlüsselungstechniken kann helfen, unerlaubten Zugriff auf sensible Daten zu verhindern.
Was denkt ihr über die Balance zwischen Datenschutz und der Bequemlichkeit digitaler Dienste?
Wir sollten auch über die potenziellen Folgen von Cyberangriffen für die Gesellschaft nachdenken und entsprechend handeln.
Es ist wichtig, dass wir unsere Kenntnisse über Cyber-Sicherheit kontinuierlich aktualisieren und verbessern.

Rollenspiel

1. Sie sind der/die IT-Sicherheitsbeauftragte eines Unternehmens. Führen Sie eine Schulung für die Mitarbeiter durch, um sie über Phishing-Attacken aufzuklären und ihnen zu zeigen, wie sie verdächtige E-Mails erkennen können.
2. Sie sind in der Leitung eines Krisenreaktionsteams in einem Unternehmen, das Opfer eines Cyberangriffs geworden ist. Koordinieren Sie die Reaktion des Teams, um die Sicherheitslücke zu identifizieren, zu schließen und die Auswirkungen auf die Unternehmensdaten zu minimieren.

CEFR
B2
C1
C2