Kapitel 11 – Risiken im Internet

Die Gefahren des Internets, die Sie kennen sollten, vor denen Sie sich in Acht nehmen sollten und mit denen Sie bei Bedarf umgehen sollten, lassen sich in 9 Kategorien einteilen.

1) **Websites mit Malware und Viren**

Beim Surfen im Internet ist es sehr leicht, auf einen falschen Link zu klicken und eine Website zu öffnen, die Malware auf Ihren Computer lädt. Wenn Sie ein aktuelles Antivirenprogramm auf Ihrem PC installiert haben, wird dieser Virus glücklicherweise fast immer gestoppt, bevor er Schaden anrichten kann. Die größte Gefahr besteht darin, nicht zu erkennen, dass Sie eine Infektion riskiert haben, die den Betrieb Ihres PCs oder die Integrität Ihrer Daten gefährden könnte. Gerade wegen der mangelnden Aufmerksamkeit vieler Menschen haben sich Ransomware-Viren wie Cryptlocker, die persönliche Dateien verschlüsseln und Lösegeld fordern, im letzten Jahr stark verbreitet.

Wir wissen, welche Websites gefährlich sind: in der Regel solche, die sich mit Piraterie, Streaming-Sites, Inhalten für Erwachsene, Dating und illegalem Material befassen. Wenn Sie es nicht vermeiden können, solche Seiten zu besuchen, sollten Sie sehr vorsichtig sein, wo Sie klicken, denn der Virus kann sich überall verstecken. Sie müssen nur auf die falsche Schaltfläche "Download" klicken, um Malware zu installieren. Und vergessen Sie nicht die Werbebanner, die Ihnen weismachen wollen, dass Ihr PC infiziert ist, obwohl das nicht der Fall ist.
Im Zweifelsfall gibt es Tools, mit denen Sie gefährliche Links und verdächtige Websites erkennen und vermeiden können.
Ein wichtiger Faktor beim Erkennen und Vermeiden von Websites mit Viren ist die Verwendung eines aktuellen Browsers, der gegen alle bisher entdeckten Bugs geschützt ist.
Zu den gefährlichsten Websites, die Malware enthalten können, gehören sicherlich Seiten für Erwachsene, Piraterieseiten jeglicher Art, fast alle Torrent-Seiten (auch mit Piraterie), illegale Download-Seiten (z.B. für Filme und Musik) und Crack-Seiten.
Wenn Sie eine solche Seite unbedingt besuchen müssen, ist es am besten, wenn Sie eine Sandbox verwenden. Sowohl in Windows 10 als auch in Windows 11 können Sie eine virtuelle Desktop-Funktion verwenden, die nicht nur ein Sicherheitstool ist, sondern auch eine großartige Möglichkeit, Dinge auf Ihrem Computer zu tun, ohne dass sie aufgezeichnet oder gespeichert werden, ähnlich wie der Inkognito-Modus von Webbrowsern. Dieses Tool heißt Sandbox und ist als eine Zone auf dem Computer gedacht, in der alles, was Sie tun, keinen Einfluss auf das System hat und sofort nach dem Schließen gelöscht wird. Die Sandbox funktioniert wie eine virtuelle Einwegmaschine, in der Sie alles, was Sie wollen, sicher ausführen können. Sie können sogar einen Virus oder eine Malware öffnen, ohne befürchten zu müssen, dass diese Ihren PC beschädigen oder Daten von Ihrem Computer stehlen.

2) Online-Privatsphäre immer in Gefahr

Es liegt auf der Hand, dass Sie einen Teil Ihrer Privatsphäre opfern müssen, wenn Sie das Internet auf partizipative Weise nutzen wollen, d.h. indem Sie sich an Foren, sozialen Netzwerken und Chats beteiligen. Auf Seiten wie Facebook ist man verpflichtet, seinen echten Namen anzugeben, während man auf anderen Seiten immer noch eine E-Mail-Adresse hinterlassen muss, über die man, wenn man möchte, den Eigentümer zurückverfolgen kann. Im Grunde kann es bei der normalen Nutzung des Internets keine Anonymität geben, und wenn jemand daran interessiert wäre, zu erfahren, wer wir sind, und über die richtigen Hacking-Fähigkeiten und Talente verfügen würde, könnte er theoretisch alles über uns wissen.

Der Schutz der Online-Privatsphäre bedeutet jedoch nicht, dass ein Hacker daran gehindert wird, unser Leben auszuspionieren, denn solange wir nicht von einem Stalker verfolgt werden oder Dinge tun, die illegal sind und versteckt werden müssen, ist es unwahrscheinlich, dass jemand seine Zeit damit verschwendet, sich in unser Leben zu hacken. Online-Privatsphäre hingegen bedeutet, dass wir einige sensible Informationen geheim halten, wie z.B. unsere Kreditkartennummern, unsere Passwörter, wo wir uns gerade aufhalten, wonach wir im Internet suchen und so weiter.

3) Ungeschützte Websites

Dies ist ein Gefahrenfaktor, der von den meisten Menschen immer noch ignoriert wird. Websites sind nicht alle gleich und werden unterteilt in sichere Websites, bei denen die von Ihnen übertragenen Informationen verschlüsselt sind und nicht von außen abgefangen werden können, und normale Websites, die unverschlüsselt übertragen.
Alle Websites, bei denen Sie ein Kennwort eingeben müssen, müssen verschlüsselt sein. Diesen Schutz erkennen Sie an dem Vorhängeschloss an der Internetadresse und dem Präfix https anstelle von http. Wenn eine Website mit HTTPS arbeitet und keine Zertifikatsfehler aufweist, sind alle von uns gesendeten Informationen, einschließlich Zugangspasswörter, Kreditkarten- oder Bankkontonummern, im Internet für niemanden sichtbar, nicht einmal für den Betreiber der Website, an die wir diese Informationen senden. Es versteht sich von selbst, dass Sie auf allen Websites mit http und ohne https keine persönlichen Daten weitergeben sollten.
Wenn Sie noch einen E-Mail-Dienst ohne https oder einen solchen oberflächlichen Online-Banking-Dienst verwenden, sollten Sie unbedingt sofort wechseln.

4) Phishing

Unter den gefährlichen Websites im Allgemeinen gibt es eine besondere Kategorie von betrügerischen Websites, wie z.B. unbekannte und nicht empfohlene Shopping-Websites

oder, noch schlimmer, gefälschte Websites, die wie bekannte Websites aussehen und erstellt wurden, um Passwörter für Konten zu stehlen.
Das Erstellen von gefälschten Websites, die Kopien von Bank- oder Shopping-Websites sind, ist eine der häufigsten Techniken, die von Hackern verwendet werden, um Passwörter für Webkonten zu stehlen, und wird als Phishing bezeichnet. Phishing funktioniert immer durch das Versenden einer Nachricht per E-Mail, Facebook, SMS, WhatsApp usw. Der beste Weg, um nicht auf diese Technik hereinzufallen, ist, sie als Vorwand für den Diebstahl von Passwörtern zu nutzen. Der beste Weg, um nicht in diese Art von Falle zu tappen, besteht darin, Passwörter und wichtige Daten (auch per E-Mail) niemals aufzuschreiben, außer auf den offiziellen Websites der Konten, erkennbar an der Adresse, die oben im Browser steht, und dem HTTPS mit grünem Vorhängeschloss.
Idealerweise sollten Sie einen E-Mail-Client wie Microsoft Outlook verwenden und einen Spam-Filter einsetzen, um diese Nachrichten zu blockieren.

5) Spam

Die Gefahr von Spam ist heute viel geringer als noch vor ein paar Jahren.
Spam ist die ganze Kategorie von Junk-Nachrichten, Werbung, Phishing und Viren oder nutzlosen Mitteilungen. Glücklicherweise verfügen die heutigen Top-E-Mail-Dienste wie Gmail und Outlook.com über einen effektiven Spam-Filter, der den Empfang von E-Mails reguliert.

6) Fehlinformationen

Auch wenn sie zur Kategorie Spam gehören, sind Fehlinformationen im Internet im letzten Jahr zu einer echten Gefahr geworden. Grund dafür ist die Verbreitung von Fake News, die wir erkennen müssen, um nicht wie Trottel dazustehen, die alles glauben, was sie im Internet oder auf Facebook lesen.

7) Online-Dating

Dies ist eine der größten Gefahren, die das Internet für junge Menschen birgt.
Es hört sich schlimm an, aber verantwortungsbewusste Eltern sollten überprüfen, ob ihre Kinder mit Fremden über das Internet chatten, egal unter welchen Umständen. Sie können mit einem Fremden in einem Online-Spiel, einer Casual-Dating-Website, einem sozialen Netzwerk, einem Forum und jedem anderen Chatroom chatten. Egal, ob es sich um sexuelle Kontakte, Verabredungen oder reine Freizeitaktivitäten handelt, es ist wichtig, dass Sie nicht zu viele persönliche Informationen preisgeben: Geben Sie nicht Ihr wahres Alter an, sagen Sie nicht, wo Sie wohnen, sagen Sie nicht, auf welche Schule Sie gehen, geben Sie keine echten Namen von Familienangehörigen oder Freunden an und geben Sie nicht Ihre Telefonnummer an. Online-Raubtiere sind sehr gut darin, sich als normale Kinder auszugeben. Sie wissen, wie sie die Schwächen von Teenagern ausnutzen können, wie es

nicht einmal die besten Psychologen können, und werden in den schlimmsten Fällen von der schrecklichen Krankheit Pädophilie getrieben.

8) Cybermobbing

Das Chatten mit Fremden kann gefährlich sein, weil man nie weiß, wer hinter der Tastatur sitzt. Aber auch das Chatten oder Messaging mit bekannten Personen kann gefährlich sein. Cybermobbing funktioniert in etwa so: Wenn Sie in der Schule oder von Ihren Freunden gehänselt werden, kann einer von ihnen ein Video oder Foto auf Facebook oder anderen sozialen Netzwerken veröffentlichen, das das Opfer in Verlegenheit bringt.
Ein weiterer Fall von Cybermobbing können anonyme Nachrichten sein, die das Opfer schwer beleidigen und sogar Drohungen enthalten.

Im Vergleich zum realen Mobber hat der Cybermobber den Vorteil, dass es keine Kontrolle gibt und er sagen kann, was er will, ohne seinem Opfer ins Gesicht zu sehen oder sich sogar anonym hinter der Tastatur zu verstecken. In beiden Fällen wäre es nicht so schwierig, zumindest auf technischer Ebene. Es ist jedoch viel komplizierter, sich auf psychologischer Ebene zu verteidigen, was die Hilfe eines Elternteils oder eines Experten erfordern kann.

9) Völlige Unkenntnis über Computersicherheit

Dies ist eine offensichtliche Gefahr, die so weit verbreitet ist, dass man sich wundert.
Ist es möglich, dass auch heute noch das häufigste Passwort der Welt 123456 ist?
Glauben die Menschen, dass, weil sie nichts zu verbergen haben, kein Hacker ihr Konto stehlen wird?
Wie kann es sein, dass Menschen immer noch für jede Website das gleiche Passwort verwenden?
Und dann gibt es immer noch Menschen, die ihre Passwörter, die vielleicht alle unterschiedlich und schwer zu merken sind, auf ein Stück Papier schreiben, das von jedem gelesen werden kann?

Dieses Projekt wird aus Mitteln der Europäischen Union kofinanziert. Die Verantwortung für den Inhalt dieses Dokuments tragen allein die Projektpartner; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Kofinanziert von der Europäischen Union

Erasmus+
Enriching lives, opening minds.