MIG-DHL

Migrants Digital Health Literacy

Handbuch

Modul 6

Digitale Kompetenz erlangen

Autoren:

Josemar Alejandro Jimenez, Oxfam; Jenny Wielga, IAT

Co-funded by the Erasmus+ Programme of the European Union

Die Unterstützung der Europäischen Kommission für die Erstellung dieser Veröffentlichung stellt keine Billigung des Inhalts dar, der ausschließlich die Ansichten der Autoren widerspiegelt, und die Kommission kann nicht für eine etwaige Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden. Projektnummer: 2020-1-DE02-KA204-007679.

Co-funded by the Erasmus+ Programme of the European Union

MIG-DHL Migrants Digital Health Literacy

Dieses Handbuch ist Teil des MIG-DHL-Programms mit insgesamt 6 Lernmodulen, das im Rahmen der strategischen Erasmus+ Partnerschaft **MIG-DHL - Migrants Digital Health Literacy** entwickelt wurde**.**

Die Ausbildungsinhalte auf einen Blick:

MIG-DHL-Programm

- Modul 1: Was ist digitale Gesundheitskompetenz und ihre Bedeutung?
- Modul 2: Die wichtigsten Gesundheitsfragen bei der Ankunft in einem neuen Land
- Modul 3: Das nationale Gesundheitssystem
- Modul 4: Digitale Kompetenz entwickeln
- Modul 5: Das nationale Gesundheitssystem im Internet erkunden
- **Modul 6: Digitale Aktivitäten zu Gesundheitsthemen**

Weitere Informationen finden Sie auf der Homepage: https://mig-dhl.eu/

Vertrag Nr. 2020-1-DE02-KA204-007679

Co-funded by the
Erasmus+ Programme
of the European Union

MIG-DHL
Migrants Digital Health Literacy

Erklärung zum Urheberrecht:

Co-funded by the
Erasmus+ Programme
of the European Union

MIG-DHL
Migrants Digital Health Literacy

Inhalt

6. Aktiv sein im digitalen Umfeld

Um im digitalen Umfeld aktiv zu sein, ist es sehr wichtig zu wissen, wie man die Privatsphäre schützt, um den Schutz persönlicher Daten im digitalen Umfeld zu verbessern und auch um die physische und psychische Gesundheit zu schützen.

Daher konzentriert sich dieses Modul auf den Schutz der Privatsphäre. Die Informationen in diesem Modul knüpfen an die Themen an, die bereits in Modul 4 behandelt wurden. Insbesondere geht es um die Entwicklung von Kompetenzen in Bezug auf Sicherheit und Datenschutz. Diese Kompetenzen beziehen sich auf die Fähigkeit, Geräte, Inhalte, persönliche Daten und die Privatsphäre in der digitalen Umgebung zu schützen. Diese Maßnahme ermöglicht auch den Schutz der körperlichen und geistigen Gesundheit, des Wohlbefindens und der sozialen Eingliederung. Dieser Teil steht im Zusammenhang mit dem Kompetenzbereich 4 "Sicherheit" von DigiComp, der bereits in Modul 4 vorgestellt wurde.

6.1 Schutz der Privatsphäre und persönlicher Daten im digitalen Umfeld

Für den Schutz der Privatsphäre und der persönlichen Daten gibt es im digitalen Umfeld eine Vielzahl von Risikofaktoren. Einige der wichtigsten Risikofaktoren, auf die auch in den Schulungsunterlagen hingewiesen wird, werden im folgenden Teil ausführlicher beschrieben.

6.1.1 Hacking

Unter Hacking versteht man Aktivitäten, die darauf abzielen, digitale Geräte wie Computer, Smartphones, Tablets und sogar ganze Netzwerke zu kompromittieren. Auch wenn Hacking nicht immer zu böswilligen Zwecken erfolgt, wird heutzutage in den meisten Fällen von Hacking und Hacker:innen gesprochen, wenn es sich um rechtswidrige Aktivitäten von Cyberkriminellen handelt, die durch finanzielle Gewinne, Proteste, das Sammeln von Informationen (Spionage) oder einfach nur durch den "Spaß" an der Herausforderung motiviert sind.

Hacker:innenangriffe sind in der Regel technischer Natur. Hacker:innen können aber auch psychologische Mittel einsetzen, um den Benutzer dazu zu bringen, auf einen bösartigen Anhang zu klicken oder persönliche Daten anzugeben.

Tatsächlich ist es zutreffend, Hacking als einen übergreifenden Oberbegriff für die Aktivitäten zu bezeichnen, die hinter den meisten, wenn nicht allen Malware- und bösartigen Cyberangriffen auf die Computeröffentlichkeit, Unternehmen und Regierungen stehen. Zu den gängigen Hacking-Techniken gehören:

- Botnetze

- Browser-Hijacks
- Denial-of-Service-Angriffe (DDoS)
- Ransomware
- Rootkits
- Trojaner
- Viren
- Würmer

Arten von Hacking/Hacker:innen

Im Großen und Ganzen kann man sagen, dass Hacker:innen aus vier Gründen versuchen, in Computer und Netzwerke einzudringen:

- Es handelt sich um kriminelle finanzielle Gewinne, d. h. den Diebstahl von Kreditkartennummern oder den Betrug an Banksystemen.
- Außerdem wollen einige Hacker:innen ihren Ruf in der Hacker:innensubkultur aufpolieren, indem sie ihre Spuren auf den von ihnen zerstörten Websites hinterlassen, um zu beweisen, dass sie den Hack durchgeführt haben.
- Dann gibt es noch die Wirtschaftsspionage, bei der die Hacker:innen eines Unternehmens versuchen, Informationen über die Produkte und Dienstleistungen eines Konkurrenten zu stehlen, um sich einen Marktvorteil zu verschaffen.

Schutz vor Hacker:innenangriffen

- Anti-Malware-Schutz: Laden Sie zuallererst ein zuverlässiges Anti-Malware-Produkt (oder eine App für das Telefon) herunter, das Malware erkennen und neutralisieren sowie Verbindungen zu bösartigen Phishing-Websites blockieren kann.
- Seien Sie vorsichtig mit Apps: Zweitens sollten Sie Telefon-Apps nur von legitimen Marktplätzen herunterladen, die sich selbst auf Malware-haltige Apps überprüfen, wie Google Play und Amazon Appstore. (Beachten Sie, dass iPhone-Benutzer laut Apple-Richtlinien nur aus dem App Store herunterladen dürfen). Trotzdem sollten Sie jedes Mal, wenn Sie eine App herunterladen, zuerst die Bewertungen und Rezensionen überprüfen. Wenn sie eine niedrige Bewertung und eine geringe Anzahl von Downloads hat, sollten Sie diese App besser meiden.
- Schützen Sie Ihre Daten: Sie sollten wissen, dass keine Bank und kein Online-Zahlungssystem Sie jemals per E-Mail nach Ihren Anmeldedaten, Ihrer Sozialversicherungsnummer oder Ihrer Kreditkartennummer fragen wird.

- Aktualisieren Sie Ihre Software: Egal, ob Sie mit Ihrem Handy oder einem Computer arbeiten, stellen Sie sicher, dass Ihr Betriebssystem auf dem neuesten Stand ist.
- Seien Sie vorsichtig: Besuchen Sie keine unsicheren Websites, laden Sie keine ungeprüften Anhänge herunter und klicken Sie nicht auf Links in unbekannten E-Mails.
- Passwortsicherheit: All das oben genannte ist grundlegende Hygiene und immer eine gute Idee. Aber die Bösewichte sind immer auf der Suche nach einem neuen Weg in Ihr System. Wenn ein/e Hacker:in eines Ihrer Passwörter entdeckt, das Sie für mehrere Dienste verwenden, hat er Apps, mit denen er in Ihre anderen Konten eindringen kann. Machen Sie also Ihre Passwörter lang und kompliziert, verwenden Sie nicht dasselbe für verschiedene Konten und nutzen Sie stattdessen einen Passwortmanager. Denn schon der Wert eines einzigen gehackten E-Mail-Kontos kann Sie ins Verderben stürzen (Malwarebytes, 2020).

6.1.2 Computerviren

Ein Computervirus ist eine der häufigsten Formen des Hackings. Ähnlich wie ein Grippevirus ist er darauf ausgelegt, sich von Wirt zu Wirt zu verbreiten und hat die Fähigkeit, sich selbst zu replizieren. Genauso wie sich Grippeviren nicht ohne eine Wirtszelle vermehren können, können sich auch Computerviren nicht ohne eine Programmierung wie eine Datei oder ein Dokument vermehren und verbreiten. Technisch gesehen ist ein Computervirus eine Art bösartiger Code oder ein Programm, das geschrieben wurde, um die Funktionsweise eines Computers zu verändern und sich von einem Computer auf einen anderen zu übertragen. Ein Virus funktioniert, indem er sich in ein legitimes Programm oder Dokument einfügt oder anhängt, das Makros unterstützt, um seinen Code auszuführen. Dabei kann ein Virus unerwartete oder schädliche Auswirkungen haben, z. B. die Systemsoftware durch Beschädigung oder Zerstörung von Daten beschädigen.

Wie greift ein Computervirus an? Sobald sich ein Virus erfolgreich an ein Programm, eine Datei oder ein Dokument angehängt hat, bleibt er so lange inaktiv, bis die Umstände den Computer oder das Gerät veranlassen, seinen Code auszuführen. Damit ein Virus Ihren Computer infizieren kann, müssen Sie das infizierte Programm ausführen, was wiederum dazu führt, dass der Viruscode ausgeführt wird. Das bedeutet, dass ein Virus auf Ihrem Computer inaktiv bleiben kann, ohne größere Anzeichen oder Symptome zu zeigen. Sobald der Virus jedoch Ihren Computer infiziert hat, kann er auch andere Computer im selben Netzwerk infizieren. Das Stehlen von Kennwörtern oder Daten, das Aufzeichnen von Tastenanschlägen, die Beschädigung von Dateien, das Versenden von Spam an Ihre E-Mail-Kontakte und sogar die Übernahme Ihres

Computers sind nur einige der verheerenden und ärgerlichen Dinge, die ein Virus anrichten kann. Während einige Viren in ihrer Absicht und Wirkung spielerisch sein können, können andere tiefgreifende und schädliche Auswirkungen haben. Dazu gehören das Löschen von Daten oder die dauerhafte Beschädigung Ihrer Festplatte. Noch schlimmer ist, dass einige Viren mit dem Ziel entwickelt werden, finanzielle Gewinne zu erzielen.

Wie verbreiten sich Computerviren? In einer ständig vernetzten Welt kann man sich auf viele Arten mit einem Computervirus infizieren, einige offensichtlicher als andere. Viren können durch E-Mail- und SMS-Anhänge, Dateidownloads aus dem Internet und betrügerische Links in sozialen Medien verbreitet werden. Ihre mobilen Geräte und Smartphones können durch fragwürdige App-Downloads mit mobilen Viren infiziert werden. Viren können sich als Anhänge von sozial geteilten Inhalten wie lustigen Bildern, Grußkarten oder Audio- und Videodateien tarnen. Um den Kontakt mit einem Virus zu vermeiden, ist es wichtig, beim Surfen im Internet, beim Herunterladen von Dateien und beim Öffnen von Links oder Anhängen Vorsicht walten zu lassen. Um sicher zu gehen, sollten Sie niemals Text- oder E-Mail-Anhänge herunterladen, die Sie nicht erwarten, oder Dateien von Websites, denen Sie nicht vertrauen.

Was sind die Anzeichen für einen Computervirus? Ein Angriff durch einen Computervirus kann eine Vielzahl von Symptomen hervorrufen. Hier sind einige von ihnen:

- Häufige Pop-up-Fenster. Pop-ups können Sie dazu verleiten, ungewöhnliche Websites zu besuchen. Oder sie fordern Sie auf, Antiviren- oder andere Softwareprogramme herunterzuladen.
- Änderungen an Ihrer Homepage. Ihre gewohnte Startseite kann sich z. B. in eine andere Website ändern. Außerdem können Sie sie möglicherweise nicht zurücksetzen.
- Massen-E-Mails, die von Ihrem E-Mail-Konto aus gesendet werden. Ein Krimineller kann die Kontrolle über Ihr Konto übernehmen oder E-Mails in Ihrem Namen von einem anderen infizierten Computer aus versenden.
- Häufige Abstürze. Ein Virus kann Ihre Festplatte stark beschädigen. Dies kann dazu führen, dass Ihr Gerät einfriert oder abstürzt. Es kann auch dazu führen, dass sich Ihr Gerät nicht mehr einschalten lässt.
- Ungewöhnlich langsame Computerleistung. Eine plötzliche Änderung der Verarbeitungsgeschwindigkeit könnte darauf hindeuten, dass Ihr Computer mit einem Virus infiziert ist.

- Unbekannte Programme, die gestartet werden, wenn Sie Ihren Computer einschalten. Möglicherweise werden Sie auf das unbekannte Programm aufmerksam, wenn Sie Ihren Computer starten. Oder Sie bemerken es, wenn Sie die Liste der aktiven Anwendungen auf Ihrem Computer überprüfen.
- Ungewöhnliche Aktivitäten wie Passwortänderungen. Dies könnte Sie daran hindern, sich bei Ihrem Computer anzumelden.

Wie kann man sich vor Computerviren schützen? Wie können Sie Ihre Geräte vor Computerviren schützen? Hier sind einige der Dinge, die Sie tun können, um Ihren Computer sicher zu halten.

- Verwenden Sie ein vertrauenswürdiges Antivirenprodukt und halten Sie es mit den neuesten Virendefinitionen auf dem neuesten Stand.
- Vermeiden Sie es, auf Pop-up-Werbung zu klicken.
- Scannen Sie E-Mail-Anhänge immer, bevor Sie sie öffnen.
- Scannen Sie immer die Dateien, die Sie mit File-Sharing-Programmen herunterladen (Norton, 2020).

6.1.3 Datendiebstahl

(beinhaltet: Assoziierter Identitätsdiebstahl, Kreditkartenkontoinformationen, Kundenreferenzen)

Datendiebstahl ist der Diebstahl digitaler Informationen, die auf Computern, Servern oder elektronischen Geräten eines unbekannten Opfers gespeichert sind, mit der Absicht, die Privatsphäre zu gefährden oder vertrauliche Informationen zu erlangen. Dabei kann es sich um finanzielle Informationen wie Kreditkartennummern oder Bankkonten handeln, aber auch um persönliche Daten wie Sozialversicherungsnummern, Führerscheinnummern und Gesundheitsdaten.

Wie kommt es zu Datendiebstahl? Datendiebstahl kann auf unterschiedliche Weise erfolgen. Meistens geschieht es, weil jemand in ein Computersystem eingedrungen ist, um vertrauliche Daten wie Ihre Kreditkarten- oder persönlichen Daten zu stehlen, oder weil ein Mitarbeiter eines Unternehmens die Daten falsch gehandhabt hat. In einer zunehmend digitalen Welt sind Hunderte von Unternehmen und Organisationen im Besitz Ihrer persönlichen Daten, z. B. Ihrer Sozialversicherungsnummer, Ihrer Postanschrift, Ihres Geburtsdatums und Ihrer Bankverbindung.

Wie können Sie sich schützen? Datendiebstahl ist ein echtes Problem, und es kann jeden treffen. Es gibt zwar keine Möglichkeit, Datendiebstahl vollständig zu verhindern, aber Sie können heute mehrere Schritte unternehmen, um Ihr Risiko zu verringern.

- Bezahlen Sie mit Bargeld statt mit Kredit- oder Debitkarten.
- Verwenden Sie eine Kredit- oder Debitkarte mit Pin-und-Chip-Technologie.
- Schützen Sie Ihren Computer vor Viren und Malware, indem Sie auf allen Ihren Computern und elektronischen Geräten Antiviren- und Anti-Spyware-Software installieren, verwenden und aktualisieren.
- Halten Sie alle Betriebssysteme und Softwareprogramme auf dem neuesten Stand, indem Sie regelmäßig Updates für Sicherheit, Webbrowser, Betriebssysteme und Softwareprogramme installieren, sobald sie verfügbar sind.
- Öffnen Sie keine fragwürdigen E-Mails oder E-Mail-Anhänge, da es sich um Phishing-E-Mails handeln könnte.
- Überprüfen Sie regelmäßig Ihre Kreditkartenabrechnungen und Ihren Kreditbericht auf nicht genehmigte Abbuchungen und neue Kreditlinien.
- Verwenden Sie ein sicheres, eindeutiges Passwort für alle Websites, die eine Anmeldung erfordern. Ändern Sie diese regelmäßig, vor allem, wenn das Passwort eines Kontos durch eine Datenpanne kompromittiert wurde.
- Verwenden Sie nur sichere Wi-Fi-Verbindungen.
- Ordnungsgemäße Entsorgung von Dokumenten mit sensiblen Informationen durch Schreddern von Papier und Entfernen aller Daten von elektronischen Geräten (Michaud, 2021).

6.1.4 Spam-Mails

Manchmal erhält man unerwünschte E-Mails - das ist einerseits zeitraubend, weil man die unerwünschten E-Mails aussortieren muss, andererseits können sogenannte Spam-E-Mails auch Gefahren wie Viren oder Schadprogramme enthalten, die sich beim Öffnen der E-Mail auf Ihrem Computer installieren und z. B. Ihre Zugangsdaten ausspähen können. Phishing ist ebenfalls eine häufige Form des Online-Betrugs, bei der Kriminelle offiziell aussehende E-Mails verschicken und versuchen, den Nutzer zur Preisgabe von Daten zu bewegen, die zum Identitätsdiebstahl verwendet werden können.

- Deshalb:

- Öffnen Sie keine Anhänge, wenn sie nicht von einem Antivirenprogramm überprüft wurden,
- Denken Sie daran, sich abzumelden, vor allem, wenn Sie einen gemeinsam genutzten öffentlichen Computer benutzen,
- Löschen Sie alle E-Mails von unbekannten Personen,
- nie auf Spam antworten.

- Wie erkennt man Spam-Mails?
  - Grammatik- und Rechtschreibfehler
  - Mails in einer Fremdsprache
  - Fehlender Name
  - Dringender Handlungsbedarf - insbesondere in Verbindung mit einer Bedrohung
  - Aufforderung zur Eingabe persönlicher Daten (z.B. PIN oder TAN)
  - Antrag auf Öffnen einer Datei
  - Noch nie eine E-Mail von der Bank erhalten oder noch nie Kunde gewesen (Verbraucherzentrale, 2021).

Literatur

Carretero, S.; Vuorikari, R. und Punie, Y. (2017). *DigComp 2.1: Der digitale Kompetenzrahmen für Bürger mit acht Kompetenzstufen und Anwendungsbeispielen*. doi:10.2760/38842

Michaud, Katelyn. (2021). *Was ist Datendiebstahl?* https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

MOZ (2022). *Google Search Operators.* https://moz.com/learn/seo/search-operators

Norman, C.; Skinner, H. (2006). eHealth Literacy: Wesentliche Fähigkeiten für die Gesundheit der Verbraucher in einer vernetzten Welt. *J Med Internet Res* 8(2):e9. DOI: 10.2196/jmir.8.2.e9

Norton. (2020). *Was ist ein Computervirus?* https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Malwarebytes. (2020). *Hacking Definition: Was ist Hacking?* https://www.malwarebytes.com/Hacker:innen

Verbraucherzentrale (2021). *Spam: E-Mail-Müll im Internet.* https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757

WebsiteSetup (2021). https://websitesetup.org/evaluating-online-resources

Weltgesundheitsorganisation [WHO]. 2017. *Digitale Gesundheitskompetenz.* https://www.who.int/global-coordination-mechanism/working-groups/digital_hl.pdf