Übung – Erkunden Ihres eigenen riskanten Online-Verhaltens

Zielsetzung

Untersuchen von Aktionen im Internet, die Ihre Sicherheit oder den Schutz Ihrer Daten gefährden können

Hintergrund/Szenario

Das Internet ist eine feindselige Umgebung, und Sie müssen wachsam sein, um Ihre Daten nicht zu gefährden. Die Angreifer sind kreativ und versuchen, Benutzer auf viele verschiedene Arten zu überlisten. In dieser Übung lernen Sie riskante Online-Verhaltensweisen kennen und erfahren, wie Sie im Internet sicherer agieren.

Teil 1: Lesen der Nutzungsbedingungen

Beantworten Sie die folgenden Fragen ehrlich, und notieren Sie die Punkte für die einzelnen Antworten. Addieren Sie sämtliche Punkte zu einer Gesamtpunktzahl, und fahren Sie mit Teil 2 fort, um Ihr Online-Verhalten zu analysieren.

a. Welche Arten von Informationen teilen Sie auf Social-Media-Websites? 3

1) Alles, ich verwende Social Media, um mit Freunden und Familienmitgliedern zu kommunizieren. (3 Punkte)
2) Artikel und Nachrichten, die ich finde bzw. lese (2 Punkte)
3) Unterschiedlich; ich achte darauf, was ich teile und mit wem. (1 Punkt)
4) Nichts, ich verwende keine Social Media. (0 Punkte)

b. Welche Aussage trifft auf Sie zu, wenn Sie ein neues Konto bei einem Online-Dienst erstellen: 2

1) Ich verwende dasselbe Passwort wie in anderen Diensten, um es mir leichter merken zu können. (3 Punkte)
2) Ich erstelle ein möglichst einfaches Passwort, um es mir leichter merken zu können. (3 Punkte)
3) Ich erstelle ein sehr komplexes Passwort und speichere es in einem Passwort-Manager-Dienst. (1 Punkt)
4) Ich verwende eine leichte Abänderung eines Passworts, das ich in einem anderen Dienst verwende. (1 Punkt)
5) Ich erstelle ein völlig neues sicheres Passwort. (0 Punkte)

c. Welche Aussage trifft auf Sie zu, wenn Sie eine E-Mail mit Links zu anderen Seiten erhalten: 4

1) Ich klicke nicht auf den Link, weil man Links in E-Mails niemals folgen darf. (0 Punkte)
2) Ich klicke auf die Links, weil diese bereits vom E-Mail-Server überprüft wurden. (3 Punkte)
3) Ich klicke auf alle Links, wenn die E-Mail von einer mir bekannten Person stammt. (2 Punkte)
4) Ich bewege den Mauszeiger über die Links, um die Ziel-URL zu überprüfen, bevor ich auf die Links klicke. (1 Punkt)

d. Beim Besuch einer Website wird ein Pop-up-Fenster angezeigt. In dem Fenster steht, dass Ihr Computer in Gefahr ist und dass Sie ein Diagnoseprogramm herunterladen und installieren sollten, um Ihren Computer zu schützen: 3

1) Ich klicke, lade das Programm herunter und installiere es, um meinen Computer zu schützen. (3 Punkte)
2) Ich untersuche das Pop-up-Fenster und bewege den Mauszeiger über den Link, um dessen Gültigkeit zu überprüfen. (3 Punkte)
3) Ich ignoriere die Nachricht, klicke nicht in das Fenster, lade das Programm nicht herunter und schließe die Website. (0 Punkte)

e. Welche Aussage trifft auf Sie zu, wenn Sie sich bei der Website Ihrer Bank anmelden: 3

1) Ich gebe meine Anmeldeinformationen sofort ein. (3 Punkte)

2) Ich überprüfe die URL, um sicherzustellen, dass ich auf der richtigen Website bin, bevor ich irgendwelche Informationen eingebe. (0 Punkte)

3) Ich verwende kein Online-Banking oder sonstige Online-Finanzdienste. (0 Punkte)

f. Sie haben von einem Programm gelesen und möchten es ausprobieren. Bei einer Online-Suche finden Sie eine Testversion auf einer unbekannten Website. Wie verhalten Sie sich? 3

1) Ich lade das Programm sofort herunter und installiere es. (3 Punkte)

2) Ich suche nach weiteren Informationen zum Entwickler des Programms, bevor ich es herunterlade. (1 Punkte)

3) Ich lade das Programm nicht herunter und installiere es nicht. (0 Punkte)

g. Auf dem Weg zur Arbeit finden Sie ein USB-Laufwerk. Wie verhalten Sie sich? 4

1) Ich nehme es mit und schließe es an meinen Computer an, um mir die Inhalte anzusehen. (3 Punkte)

2) Ich nehme es mit, schließe es an meinen Computer an und lösche sämtliche Daten, bevor ich es selbst verwende. (3 Punkte)

3) Ich nehme es mit, schließe es an meinen Computer an und führe ein Antivirusprogramm aus, bevor ich es für meine eigenen Dateien verwende (3 Punkte).

4) Ich nehme es nicht mit. (0 Punkte)

h. Sie benötigen Zugriff auf das Internet und finden einen offenen Wi-Fi-Hotspot. Wie verhalten Sie sich? 2

1) Ich verbinde mich mit dem Hotspot und nutze das Internet. (3 Punkte)

2) Ich verbinde mich nicht mit dem Hotspot und warte stattdessen, bis ich eine vertrauenswürdige Verbindung nutzen kann. (0 Punkte)

3) Ich verbinde mich mit dem Hotspot und stelle eine VPN-Verbindung mit einem vertrauenswürdigen Server her, bevor ich irgendwelche Daten übertrage. (0 Punkte)

Teil 2: Analysieren Ihres Online-Verhaltens

Je höher Ihre Punktzahl ist, desto riskanter ist Ihr Online-Verhalten. Das Ziel ist 100%ige Sicherheit, indem Sie bei sämtlichen Online-Interaktionen sehr vorsichtig sind. Dies ist sehr wichtig, da ein Fehler ausreicht, um Ihren Computer und Ihre Daten zu gefährden.

Addieren Sie die Punkte aus Teil 1. Notieren Sie Ihre Punktzahl. 5

0: Sie sind online extrem sicher.

0 - 3: Sie sind online relativ sicher, können Ihr Verhalten und damit Ihre Sicherheit jedoch noch weiter verbessern.

3 - 17: Ihr Online-Verhalten ist unsicher, und es besteht ein hohes Risiko, dass Sie dadurch Ihre Daten gefährden.

18 oder mehr: Ihr Online-Verhalten ist sehr unsicher, und Ihre Daten sind definitiv gefährdet. Hier finden Sie einige praktische Tipps für die Online-Sicherheit.

a. Je mehr Informationen Sie auf Social-Media-Websites teilen, desto mehr kann ein Angreifer über Sie erfahren. Mit diesem Wissen können Angreifer spezielle, zielgerichtete Angriffe planen. Wenn Sie der Welt zum Beispiel mitteilen, dass Sie ein Autorennen besucht haben, kann ein Angreifer Ihnen eine bösartige E-Mail schicken, die so aussieht, als käme sie von dem für das Rennen verantwortlichen Ticketunternehmen. Die E-Mail erscheint glaubwürdiger, da Sie das Event tatsächlich vor Kurzem besucht haben.

b. Vermeiden Sie es, Passwörter wiederzuverwenden. Wenn Sie ein Passwort in einem Dienst wiederverwenden, der unter der Kontrolle eines Angreifers steht, kann sich dieser Angreifer unter Umständen bei anderen Diensten mit Ihrem Namen anmelden.

c. E-Mails können sehr leicht gefälscht werden. Gefälschte E-Mails enthalten häufig Links zu bösartigen Websites oder Malware. Klicken Sie generell nicht auf eingebettete Links, die Sie per E-Mail erhalten.

d. Akzeptieren Sie niemals Software, die Sie nicht angefordert haben, ganz besonders nicht auf Websites. Es ist extrem unwahrscheinlich, dass Sie auf einer Website ein legitimes Softwareupdate erhalten. Schließen Sie in diesem Fall Ihren Browser, und verwenden Sie die Tools Ihres Betriebssystems, um nach den Updates zu suchen.

e. Bösartige Websites können mühelos gefälscht werden, um das Aussehen einer Bank-Website zu kopieren. Überprüfen Sie stets die URL, um sicherzustellen, dass Sie auf der richtigen Seite sind, bevor Sie auf Links klicken oder irgendwelche Informationen eingeben.

f. Wenn Sie die Ausführung eines Programms auf Ihrem Computer erlauben, geben Sie ihm damit umfangreiche Berechtigungen. Überlegen Sie sich gut, welche Programme auf Ihrem Computer ausgeführt werden dürfen. Vergewissern Sie sich, dass das Unternehmen bzw. die Einzelperson hinter dem Programm seriös und legitim ist. Laden Sie Programme nur von der offiziellen Website des Unternehmens bzw. der Person herunter.

g. USB-Laufwerke und -Sticks enthalten einen Mikrocontroller, um mit Computern kommunizieren zu können. Dieser Controller kann infiziert und angewiesen werden, bösartige Software auf dem Host-Computer zu installieren. Da die Malware im USB-Controller selbst gehostet wird und nicht im Datenbereich, wird sie bei der Löschung oder Virenprüfung nicht erkannt.

h. Angreifer verwenden häufig gefälschte Wi-Fi-Hotspots, um Benutzer anzulocken. Da der Angreifer Zugriff auf alle über den präparierten Hotspot übertragenen Daten hat, sind sämtliche mit dem Hotspot verbundenen Benutzer in Gefahr. Verwenden Sie niemals unbekannte Wi-Fi-Hotspots, ohne Ihre Daten mit einem VPN zu verschlüsseln. Geben Sie niemals sensible Daten wie z. B. Kreditkartennummern ein, während Sie mit einem unbekannten Netzwerk (kabellos oder kabelgebunden) verbunden sind.

Überlegung

Welche Änderungen würden Sie nach dieser Analyse an Ihrem Online-Verhalten vornehmen, um sich besser zu schützen?

Einen Password-Manager nutzen.
Aktuell belegte Passwörter ändern.

