Safety-Buzzwords

Im Bereich Datenschutz findet man sich schnell mit vielen – in Teilen sehr kryptisch klingenden – Fachwörtern, die nicht selten aus dem Englischen entstammen, konfrontiert. Um Strategien zum Schützen der digitalen Arbeitsumgebung besser verstehen oder auch identifizieren zu können, ist es sinnvoll, sich einmal mit diesen Fachbegriffen auseinandergesetzt zu haben.

Im vor euch liegenden Stapel findet ihr Begriffskarten mit diversen Fachwörtern. Zieht nacheinander zufällig einen von den Begriffen und überlegt gemeinsam, was das Wort bedeuten könnte. Dann notiert ihr auf dem ausliegenden Flipchart, ob ihr den Begriff kanntet oder ob ihr zum Verständnis erst ein wenig recherchieren musstet. Wiederholt das beliebig oft. Vielleicht fallen euch ja auch noch weitere Begriffe ein, die ihr auf dem Flipchart ergänzen könnt.

Scammer	Passwort-Manager	Privacy	Phishing	Backup
PGP Key	Firewall	Antiviren-programm	Catfishing	Chatbot
Zwei-Faktor-Authentifi-zierung	Encryption	Cookies	Metadaten	Geoblocking
Profiling	VPN	DSGVO	BCC	Bot
Scam	Zählpixel	Ransom-ware	Zero-Click Attacke	

Passwort-Merk-Spiel

An dieser Station tretet ihr gegeneinander an: Wer von euch kann sich das sicherste Passwort ausdenken und merken? Dazu braucht ihr **Zettel**, **Stift** und eine **Stoppuhr**.

Lest euch **zuerst die Arbeitsanleitung** komplett durch. Zückt danach einen Zettel und Stift pro Person. Startet die Stoppuhr, sobald ihr bereit seid.

Wenn ihr fertig seid, könnt ihr euch überlegen, welche Strategie für ein sicheres Passwort die beste war. Haltet diese auf dem ausliegenden Flipchart fest. Gerne könnt ihr auch eine Hitliste der eurer Meinung nach unsichersten Passwörter aufschreiben.

Anleitung

1) Jede:r von euch hat **30 Sekunden Zeit**, um sich ein möglichst starkes Passwort auszudenken, auf den Zettel aufzuschreiben und auch einzuprägen.

2) Sind die **30 Sekunden vorbei**, dreht ihr eure Zettel um und legt sie vor euch hin.

3) Jetzt habt ihr **2 Minuten Zeit**, um nicht an euer Passwort zu denken. Unterhaltet euch zum Beispiel über die lustigste Spammail, die ihr je erhalten habt.

4) Danach habt ihr 15 Sekunden, um das von euch **gemerkte Passwort auswendig auf einen Zettel aufzuschreiben** (ohne unter den umgedrehten Zettel zu gucken, selbstverständlich).

5) Jetzt könnt ihr die **Zeit anhalten** und überprüfen, ob ihr euch euer Passwort richtig gemerkt habt.

6) Gebt gemeinsam die Passwörter auf der Webseite wiesicheristmeinpasswort.de ein, die ihr im 4. Schritt aufgeschrieben habt.

7) Die Webseite verrät euch, wie lange ein Computer bräuchte, um euer Passwort zu knacken. Außerdem könnt ihr einsehen, aus welchen „Bausteinen“ sich euer Passwort zusammensetzt, nach denen ein Programm zum Passwortknacken Ausschau hält.

8) Das Passwort, für das ein Computer am längsten bräuchte, ist das sicherste und gewinnt, vorausgesetzt, ihr habt es euch richtig gemerkt.

wie sicher ist mein Passwort .de

Passwort-Sicherheits-Check

Phishing erkennen

Unter *Phishing* versteht man betrügerische Versuche, auf digitalem Weg an Daten oder Geld heranzukommen. Das passiert beispielsweise mittels gefälschter E-Mails, Kurznachrichten, oder Webseiten. Viele Phishing-Versuche bekommt ihr zum Glück nur in dem Spam-Ordner eures E-Mail-Accounts zu sehen, da sie automatisch als unecht erkannt werden. Viele dieser Nachrichten sind oft sogar sehr amüsant.

In diesem kleinen Quiz von *Google* könnt ihr testen, wie gut ihr Phishing-Mails von ungefährlichen Mails unterscheiden könnt. Wenn ihr wollt, könnt ihr auch gegeneinander antreten und schauen, wer von euch der:die Phishing-Expert:in wird.

phishingquiz.withgoogle.com/?hl=de

Wenn ihr fertig seid, könnt ihr überlegen, welche Strategie(n) ihr verwendet, um Phishing-Mails von echten Mails zu unterscheiden. Ergänzt diese auf der ausliegenden Mindmap. Wenn ihr möchtet, schreibt eure persönliche Hitliste der absurdesten Phishing-Mail-Maschen auf.

Wie sicher ist dein digitales Ich?

Wie sicher ist dein digitales Ich? Diese Frage stellt dir das Online-Magazin für digitale Freiheitsrechte *netzpolitik.org*. Durch 10 Fragen wird dein persönlicher Privacy-Score berechnet. Es geht bei diesem Quiz weniger darum, euch anschließend zu vergleichen, wer die meisten Punkte erreicht hat. Vielmehr soll ein wenig das eigene Verhalten reflektiert und ein Verständnis entwickelt werden, welche Faktoren einen Einfluss auf den erreichten Score haben.

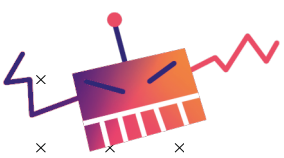
Wenn ihr fertig seid, könnt ihr euch überlegen, welche Auswirkung die Nutzung bestimmter Medien im Arbeitsalltag auf euren Datenfußabdruck hat. Danach könnt ihr Tipps zum Schützen der persönlichen Daten im Netz auf der ausliegenden Mindmap ergänzen.

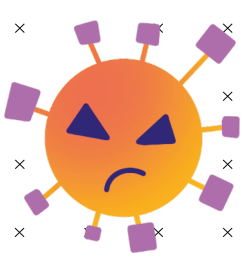
Twitter-Wettrennen: Privatsphäre Einstellungen

In den Einstellungen deines Social-Media-Accounts kann man weitaus mehr ändern als nur die Sprache oder das eigene Passwort. An dieser Station sollt ihr ein wenig in die Einstellungen eines *Twitter*-Accounts eintauchen – verpackt in einem kleinen Suchspiel.
Jede:r von euch benötigt ein eigenes Endgerät. Wenn ihr ein kleines Wettrennen daraus machen wollt, solltet ihr zunächst sicherstellen, dass ihr mit den gleichen Startvoraussetzungen antretet. Dazu gehören bspw. die gleiche *Twitter*-Anwendung (App oder Browser, iOS oder Android bspw.) auf eurem Endgerät, den gleichen Internetzugang und am besten ein möglichst unkonfigurierten *Twitter*-Account.

Anleitung
Vor euch findet ihr kleine Zettel (noch sind sie allerdings umgedreht). Darauf befinden sich 5 kleine Suchaufträge, die ihr in den „Einstellungen" eures *Twitter*-Accounts finden könnt.
Wenn ihr bereit seid, könnt ihr gemeinsam die Zettel umdrehen und so schnell wie möglich versuchen, euch an die Orte in den entsprechenden Einstellungen zu navigieren. Gefunden? Das ist gut, jetzt schreibt ihr euch entweder den entsprechenden Pfad auf einen Zettel oder ihr macht einen Screenshot als „Beweis", dass ihr die Aufgabe erfüllt habt.
Wer zuerst alle 5 Einstellungen gefunden hat, gewinnt das *Twitter*-Wettrennen. Wenn ihr möchtet, könnt ihr eure Zeit stoppen und euer Ergebnis auf dem Flipchart festhalten. Dann solltet ihr für die nächste Gruppe noch die Aufgabenzettel wieder umdrehen.

Wenn ihr damit fertig seid, könnt ihr auf dem ausliegenden Flipchart eure persönlichen Empfehlungen für „Das solltet ihr unbedingt in den Einstellung eures Sozialen-Netzwerks festlegen" ergänzen.





Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Security Risks Game

Herumliegende Festplatten oder unverschlüsselte Tablets, die mit wichtigen Daten gefüllt sind, werden meistens erst dann zum Problem, wenn sie in die falschen Hände geraten. Der Teufel steckt wie so oft im Detail. Dieses kleine Wimmelbild-Spiel sensibilisiert für jene Details, die im eigenen Arbeitsalltag potenzielle Sicherheitslücken darstellen.

Besucht die folgende – leider nicht für Touchscreen-Bildschirme optimierte – Webseite und schult eure Wahrnehmung für solche Sicherheitslücken. Ihr könnt gegeneinander antreten und schauen, wer von euch schneller ist oder gemeinsam versuchen, einen Überblick zu bekommen: hotspot.livingsecurity.com

Da die Webseite auf Englisch ist, solltet ihr schauen, dass keine:r allein den Sprachbarrieren ausgesetzt ist und dass ihr am Ende die Ergebnisse besprecht.
Wenn ihr fertig seid, dürft ihr euren (Gruppen-)Highscore, die Zeit, die ihr gebraucht habt, und die gefundenen Dinge auf dem ausliegenden Flipchart in eine Liste ergänzen. Danach könnt ihr gemeinsam überlegen, welche potentiellen Sicherheitslücken euch noch einfallen oder welchen davon ihr vielleicht im Alltag begegnet. Ergänzt diese ebenfalls auf dem Flipchart und fügt auch ein paar Strategien zum Verhindern dieser Sicherheitslücken hinzu, sofern euch welche einfallen.