



REMCREAD

Empowering Refugee & Migrant Women
through Creative Methods and Digital Literacy

ماژول 3:

ایمینی و حریم خصوصی آنلاین

طرح درس



Co-funded by
the European Union

توسط اتحادیه اروپا تامین مالی می شود. با این حال، دیدگاه ها و نظرات بیان شده فقط متعلق به نویسنده (ها) است و لزوما منعکس کننده نظرات اتحادیه اروپا یا آژانس اجرایی آموزش و فرهنگ اروپا (EACEA) نیست. نه اتحادیه اروپا و نه EACEA نمی توانند مسئول آنها باشند.

شماره پروژه PL01-KA220-ADU-000156610-1-2023

وب سایت پروژه [/https://www.remcreadwomen.eu](https://www.remcreadwomen.eu)

ماژول 3. امنیت و حریم خصوصی در وب

مقدمه

ماژول "ایمنی و حریم خصوصی آنلاین" به عنوان یک منبع آنلاین تعاملی توسعه یافته است که در: [ایمنی و حریم خصوصی آنلاین](#) موجود است. از این منابع می توان به روش های مختلفی استفاده کرد - به عنوان ارائه در طول یک جلسه کلاسی، به عنوان بخشی از یک دوره آموزش الکترونیکی یا در قالب یادگیری ترکیبی، ترکیبی از کار آنلاین و آفلاین.

هدف از این ماژول افزایش آگاهی شرکت کنندگان در مورد حفاظت از داده ها، استفاده ایمن از رسانه های اجتماعی و به حداقل رساندن خطرات مرتبط با فعالیت آنلاین است. این مطالب شرکت کنندگان را گام به گام از درک ماهیت امنیت آنلاین، از طریق مهارت های عملی (از جمله ایجاد رمزهای عبور قوی، پیگیری تنظیمات حریم خصوصی، استفاده از 2FA) تا انتشار آگاهانه محتوا و پاسخ به نقض حریم خصوصی راهنمایی می کند.

ساختار ماژول بر اساس یک طرح درسی است که شامل موارد زیر است:

- مقدمه ای بر امنیت و حریم خصوصی،
- خطرات مرتبط با رسانه های اجتماعی (سرقت داده ها، فیشینگ، تعقیب سایبری، جعل، اعتیاد)،
- اصول ورود ایمن و استفاده از شبکه های Wi-Fi عمومی،
- عواقب انتشار داده های شخصی، عکس ها و اطلاعات مکان،
- مطالعه موردی و تمرینات گروهی،
- خلاصه و منابع و ابزارهای اضافی.

منابع آنلاین شامل فیلم ها ، گرافیک ها ، پیوندهایی به منابع خارجی و تمرینات توصیف شده است که می توانند به صورت جداگانه یا گروهی انجام شوند. این راهنما همچنین راهنمایی هایی را در مورد نحوه انجام بحث ها و مطالعات موردی برای درگیر کردن شرکت کنندگان و کمک به آنها در انتقال دانشی که به دست آورده اند به تجربیات آنلاین خود ارائه می دهد.

به لطف قالب انعطاف پذیر، مطالب را می توان هم در نسخه کامل (تقریباً 120 دقیقه) و هم در نسخه کوتاه شده متناسب با ظرفیت زمانی گروه تحویل داد. مربی با در نظر گرفتن نیازها و سطح شایستگی شرکت کنندگان تصمیم می گیرد که کدام عناصر را شامل شود.

ایمنی و حریم خصوصی آنلاین

ماتریس شایستگی امنیت دیجیتال برای یک فرد فعال در رسانه های اجتماعی

نگرش	مهارت	دانش	حوزه شایستگی
- مراقبت از استفاده از رمزهای عبور مختلف برای حساب های مختلف - اعتماد به ابزارهای مدیریت رمز عبور - احتیاط در اشتراک گذاری رمزهای عبور	- ایجاد و تغییر رمزهای عبور قوی - پیکربندی 2FA در پلتفرم های مختلف - پشتیبانی از مدیر رمز عبور	- اصول ایجاد رمزهای عبور قوی - نقش مدیران رمز عبور - اهمیت 2FA	مدیریت رمز عبور
- رویکرد انتقادی به پیام های دریافتی - احتیاط در ارائه داده ها - هوشیاری نسبت به موقعیت های غیرمعمول	- تشخیص پیامها و سایتهای مشکوک - گزارش فیشینگ - محافظت از اطلاعات شخصی	- انواع حملات فیشینگ - تکنیک های مهندسی اجتماعی - مورد استفاده مجرمان سایبری	آگاهی از فیشینگ و مهندسی اجتماعی
- به روز نگه داشتن نرم افزار - آگاهی از خطرات مرتبط با عدم امنیت - مسئولیت دستگاه های خود	- نصب و پیکربندی آنتی ویروس - به روز رسانی منظم نرم افزار - دستگاه های ایمن سازی	- نقش به روز رسانی سیستم - اهمیت آنتی ویروس و فایروال - تهدیدات مرتبط با دسترسی فیزیکی به دستگاه ها	امنیت دستگاه ها
- احترام به حریم خصوصی خود و دیگران - مسئولیت داده های در حال پردازش - آگاهی حقوقی مربوط به حفاظت از داده ها	- تنظیمات حریم خصوصی را پیکربندی کنید - محدود کردن دید اطلاعات شخصی - به اشتراک گذاری ایمن اطلاعات	- تنظیمات حریم خصوصی در پلتفرم ها - حفاظت از داده ها - مقررات (GDPR) (RODO).	مدیریت داده ها و حریم خصوصی
- هنگام استفاده از شبکه های عمومی احتیاط کنید - فعال بودن در ایمن سازی اتصالات - آگاهی از تهدیدات آنلاین	- پیکربندی VPN - استفاده ایمن از شبکه های Wi-Fi - اجتناب از اتصالات اینترنتی خطرناک	- خطرات شبکه های Wi-Fi عمومی - ویژگی ها و مزایای استفاده از VPN	استفاده ایمن از شبکه ها

مدیریت حساب و محتوا	- ابزارهای نظارت بر حساب - نقش سیاست های حفظ حریم خصوصی در رسانه های اجتماعی	- بررسی و تجزیه و تحلیل - منظم فعالیت حساب - انتشار ایمن محتوا	- مسئولیت مطالب منتشر شده - توجه به رعایت سیاست های حفظ حریم خصوصی - فعال بودن در نظارت بر فعالیت
---------------------	---	--	---

ماژول 3. امنیت و حریم خصوصی در وب

نتایج یادگیری:

شرکت کنندگان در کارگاه:

- درک کنید که چرا حریم خصوصی و امنیت آنلاین مهم است.
- قادر به ایجاد رمزهای عبور قوی و استفاده از احراز هویت دو مرحله ای هستند.
- قادر به تنظیم سطوح مناسب از حریم خصوصی در پروفایل های اجتماعی خود هستند.
- از خطرات ناشی از انتشار داده های شخصی، عکس ها و مکان ها آگاه باشند.
- بدانید که چگونه از شبکه های Wi-Fi عمومی و دستگاه های عجیب و غریب با خیال راحت استفاده کنید.
- بدانید که در صورت نقض حریم خصوصی یا تصاحب حساب چگونه پاسخ دهید.
- می توانند ارزیابی کنند که چه محتوایی برای ارسال در رسانه های اجتماعی بی خطر است.

مدت زمان: 120 دقیقه

منابع دیگر / پیوند به منابع	زمان	مواد	یادداشت های روش شناختی	هدف	فعالیت
https://sites.google.com/view/safety-and-privacy-remcread-en	15 دقیقه	محتوا از https://sites.google.com/view/safety-and-privacy-remcread-en - داستان مگدا، کریستوفر ، نمونه های مربی. -	معرفی مختصر توسط مربی + مثال های واقعی	افزایش آگاهی از خطرات آنلاین و پیامدهای آن.	1. مقدمه: چرا حریم خصوصی آنلاین مهم است؟
دستورالعمل ایجاد رمزهای عبور قوی و پیکربندی 2FA	15 دقیقه	تخته سفید/فلیپ چارت، نشانگر، برنامه های تلفن همراه	نمایش گام به گام	شرکت کنندگان یاد خواهند گرفت که چگونه رمزهای عبور قوی	2. رمزهای عبور قوی و 2FA

	ایجاد کنند و اهمیت احراز هویت دو مرحله ای را درک کنند.	فیلم پیشنهادی که به زبان انگلیسی است را می توان با استفاده از تنظیمات یوتیوب ترجمه کرد. مطالب پیشنهادی در قالب صفحات وب را می توان با استفاده از مترجم در مرورگری مانند Chrome به هر زبانی ترجمه کرد. برای بهترین ترجمه پیشنهاد می شود از صفحه تهیه شده در پروژه به زبان انگلیسی استفاده کنید.			چگونه از حساب های خود محافظت کنیم احراز هویت دو مرحله ای چیست؟ احراز هویت چیست؟ احراز هویت دو مرحله ای 2FA: زندگی دیجیتال خود را ایمن کنید مدیر رمز عبور چیست آیا به آن نیاز دارم؟
20 دقیقه	دسترسی به اینترنت، دستورالعمل های YouTube	کار فردی با تلفن / لپ تاپ + پشتیبانی مربی.	شرکت کنندگان به طور مستقل تنظیمات حساب خود را بررسی و تغییر می دهند.	3. تنظیمات حریم خصوصی نمایه	نحوه بیکر بندی حریم خصوصی در اینستاگرام
15 میت	محتوا از https://sites.google.com/view/safety-and-privacy-remcread-en	بحث هدایت شده، تجزیه و تحلیل مثال ها.	شرکت کنندگان می توانند تشخیص دهند که کدام محتوا برای انتشار بی خطر است.	4. اشتراک گذاری آگاهانه محتوا	حریم خصوصی و رسانه های اجتماعی
15 دقیقه	محتوا از https://sites.google.com/view/safety-and-privacy-remcread-en	ارائه + سوالات به گروه	شرکت کنندگان خطرات مرتبط با Wi-Fi عمومی و نحوه اجتناب از آنها را می دانند.	5. ورود ایمن و استفاده از Wi-Fi	مبانی امنیت سایبری - آموزش و محافظت از خود

6. در صورت نقض حریم خصوصی چه باید کرد؟	شرکت کنندگان مراحل را که باید پس از تصاحب حساب انجام دهند، می دانند.	بحث، تجزیه و تحلیل رویه ها	توضیحات رویه ها (فیس بوک، اینستاگرام، توئیتر ایکس)	15 دقیقه	https://help.instagram.com/
7. مطالعه موردی: ماریا و امنیت زنان پناهنده	تأمل در مورد ایمنی کاربران آسیب پذیر.	کار گروهی + ارائه نتیجه گیری	گزارش موردی ماریا https://sites.google.com/view/safety-and-privacy-remcread-en	20 دقیقه	
8. خلاصه و سوالات	برجسته کردن اصول کلیدی و رسیدگی به نگرانی ها.	سوالات باز، مجموعه ای از نتیجه گیری ها		5 دقیقه	