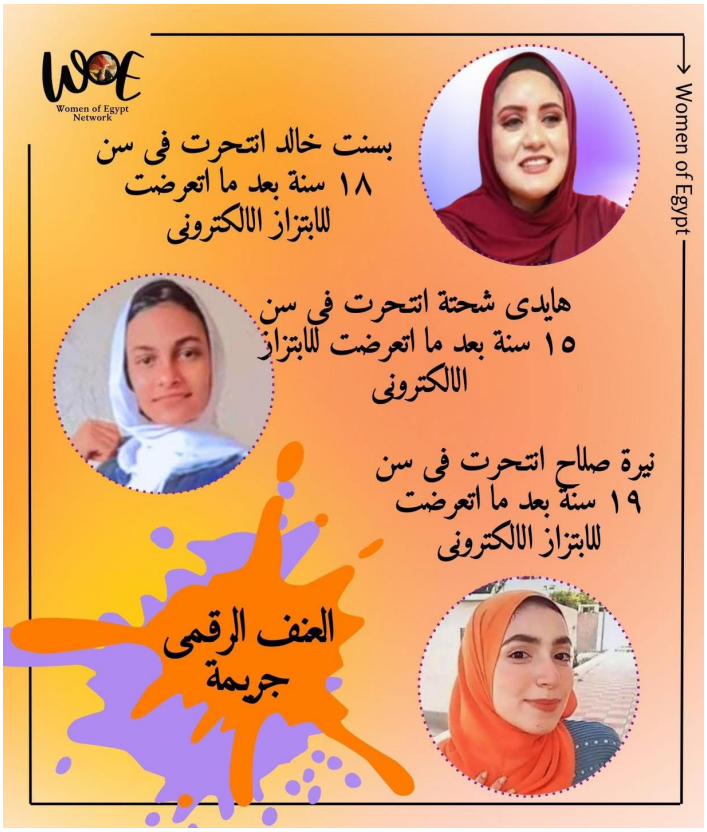
كتيب السلامة الرقمية
سلامة رقمية كلينيك

دليل السلامة الرقمية و كيفية الحماية من العنف الرقمي

المحتوي

مقدمه



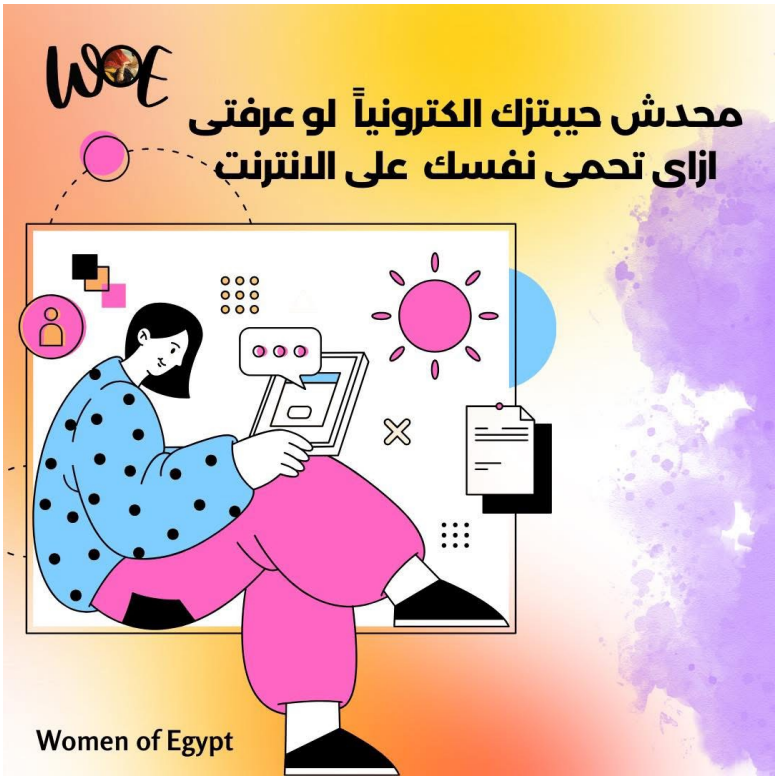
بسنت خالد، وهايدى شحتة ونيرة صلاح؛ التلاتة ضحايا للعنف الرقمى. التلاتة انتحروا بعد ما تعرضوا لتهديد وابتزاز على الانترنت، ودول نوع من أنواع العنف الرقمى.

المجرمين سرقوا صور بسنت خالد وهايدى شحته من على حسابهم على السوشال ميديا وفبركوها؛ وبالنسبة لنيرة صلاح، زميلتها فى السكن فى الجامعة سرقت صور ومحادثات خاصة من تليفون نيرة وهددتها انها حتنشرها.

اللى تسببوا فى انتحار البنات اخدوا جزاتهم، لأن الابتزاز الالكترونى جريمة ولها عقاب؛ ولكن للاسف الـ ٣ بنات ضاعت حياتهم علشان خافوا يبلغوا، وخافوا من كلام الناس، وخافوا من المجتمع، وخافوا من اهلهم ... مع ان محضر للشرطة كان ممكن يساعدهم ياخدوا حقهم.

العنف الرقمي هو لما الناس يستخدموا التكنولوجيا زي الإنترنت السوشال ميديا عشان يسببوا اذى احد. العنف الرقمى له أشكال كتير، زي التحرش على الإنترنت، والتشهير على السوشال ميديا، او الابتزاز ؛ او اى فعل مؤذى بيتم باستخدام التليفون او جهاز اللآب توب.

إزاي تحمى نفسك من الابتزاز الالكترونى؟



الإنترنت أصبح جزء أساسي من حياتنا، وعلشان كده مهم نعرف ازاى نحافظ على سلامتنا الرقمية، علشان بياناتنا متتسرقش ونتعرض للتحرش الابتزاز الالكترونى. ممكن نحمى نفسنا بشوية خطوات بسيطة.

- متديش بياناتك الشخصية لحد
- اظبطى إعدادات الخصوصية للمواقع اللى بتزوريها
- استخدمى جوجل لما تحبى تدورى على حاجة على الانترنت علشان ده من المواقع الآمنة
- خلى بالك قبل ما تعملى داونلود لأى لينك بيوصلك فى ايميل او مسيدج.
- اختارى كلمة مرور (كلمة سر) قوية، مكونة على الاقل من ٨ رموز وأرقام
- خلى بالك جدا من "الفيشينج" او التصيد، خصوصا فى الايميل والمسيدچيز على وسائل التواصل الاجتماعي.

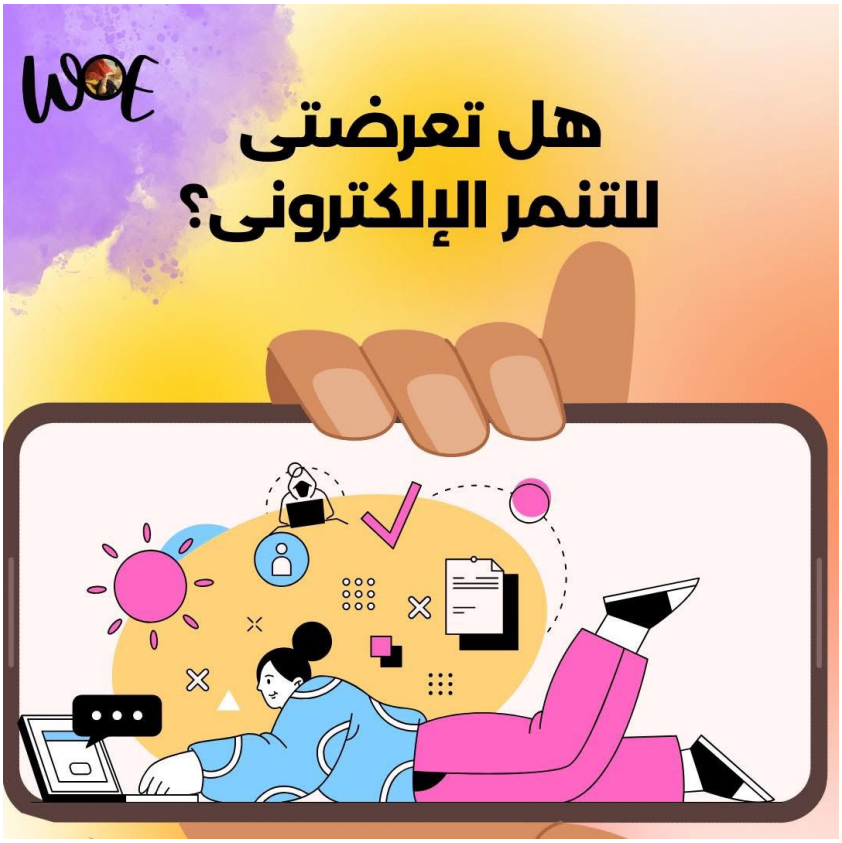
⭕ اشترى من مواقع معروفة وموثوق فيها.

⭕ خلى بالك قبل ما تدوس على اى لينكات (روابط) عشان ممكن تكون فيها فيروسات.

⭕ اعملى تحديث باستمرار لأجهزتك

⭕ احتفظى بنسخة احتياطى من كل بياناتك وكلمات المرور

تعريف التنمر الألكتروني



التنمر الإلكتروني هو استخدام التكنولوجيا عشان نضايق أو نخوف أو نهدد أو نفضح حد.

⭕ التنمر الالكترونى بيحصل على السوشال ميديا؛ زى فيسبوك، إنستجرام، سناب شات، وتيك توك، او على المسينجر او واتس اب او تليجرام او على الموبايل؛ وغيرها من التطبيقات دى.

⭕ وده بيكون فى شكل نشر قصص كاذبة او مسيئة عن شخص معين؛ أو نشر صور وفيديوهات شخصية ممكن تسبب لها الحرج.

⭕ وممكن كمان بيكون فى شكل مسيدچات فيها كلام او صور أو فيديوهات مؤذية أو مسيئة أو فيها تهديد.

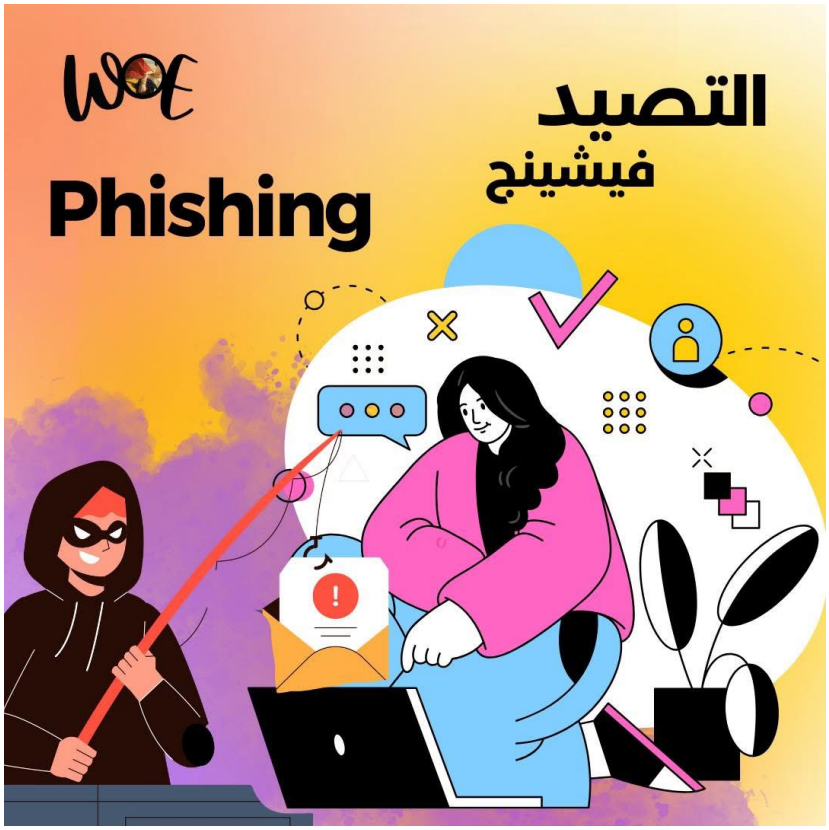
⭕ المتنمر ملهوش هدف تانى غير الأذية؛ سواء نفسية او معنوية أو مادية.

⭕ مهم نعرف ان التنمر الالكترونى فى اى شكل من اشكاله سواء رساله او صور او ڤيديو او رسالة مسجلة، ممكن نستخدمهم كلهم دليل ضد المتنمر.

⭕ لو في حد بيتنمر عليكي، أول حاجة لازم تعمليها هي انك تطلبي المساعدة من حد تثقي فيه زي مامتك او باباكى أو حد في العيلة، او مُدرسة تثقى فيها.

⭕ ولو كان التنمر بيحصل على السوشال ميديا، خدى سكرين شوت بالرسائل اللى وصلت لك؛ واعملى بلوك (حظر) للشخص ده وبلغى عنه الفيس بوك او انستجرام او تيك توك، او اى منصة تانية تعرضتى فيها للتنمر

التصيد



الهاكرز كل يوم بيخترعوا طرق جديدة علشان يخترقوا حسابات ويستخدموا المعلومات اللي بيسرقوها في ايذاء أصحاب الحسابات دي.

الـ PHISHING او التصيد، أصبح من أكتر الحيل اللي بيستخدمها الهاكرز لإختراق الحسابات، وللأسف بيستخدموا تقنية عالية أحيانا بيكون من الصعب كشفها.

ازاي بيتم اختراق الحسابات من خلال الـ Phishing ؟

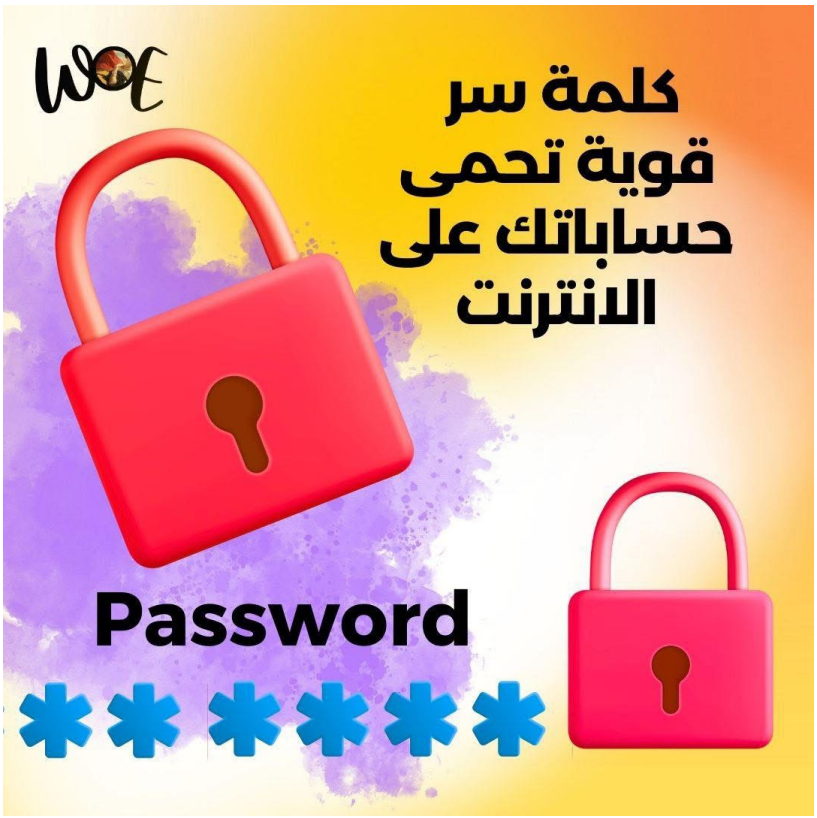
بيوصلك ايميل من شركة مشهورة أو بنك، بيحذرك ان حسابك حيتقفل، او إنك كسبت خدمة أو فلوس، أو ان عليك فلوس لهم، أو أي طريقة تانية يحاولوا فيها انهم يوجهوكي انك تضغطي علي رابط موجود في الإيميل.

وفي الرابط ده بيطلبوا منك انك تحطى الباسوورد او رقم الكريديت كارد. الروابط دي بتوصل جهازك لمواقع بيقدروا من خلالها سرقة بياناتك.

علشان تحمي حسابك من الإختراق، بلاش تضغطي علي الروابط في رسائل البريد الإلكتروني اللي بتوصل من أشخاص مجهولين؛ علشان ده ممكن يعرض جهازك للخطر.

وفي حالة لو وصلك لينك في ايميل من حد تعرفيه، مش حتخسروا حاجة لو اتأكدتم بنفسكم من صاحب الايميل انه هو فعلا اللي بعته قبل ما تضغطوا علي اللينك، لانه هو نفسه ربما يكون كمان حسابه تم اختراقه، والهاكرز بيبعتوا ايميلات لأصحابه علشان يخترقوا حساباتهم هم كمان .

ازاى تختارى كلمة سر قوية؟



🔴 إختيار كلمة سر password قوية هي أول حاجة بنقدر نحمي بيها بياناتنا وحساباتنا على الإنترنت

⭕ استخدمي دائما خليطاً من الأحرف والأرقام والرموز

⭕ وكل ما تكون طويلة كان افضل (متقلش عن ١٦ حرف) Dg1@-XF-$OL?2639

⭕ استخدمى كلمة سر مختلفة لكل حساب (علشان لو حصل تهكير لحساب، الهاكر ميقدرش يوصل لباقي الحسابات).

⭕ بلاش تستخدمي معلومات شخصية فى كلمة السر، يعنى بلاش رقم تليفونك ولا عيد ميلادك ولا اسماء اولادك

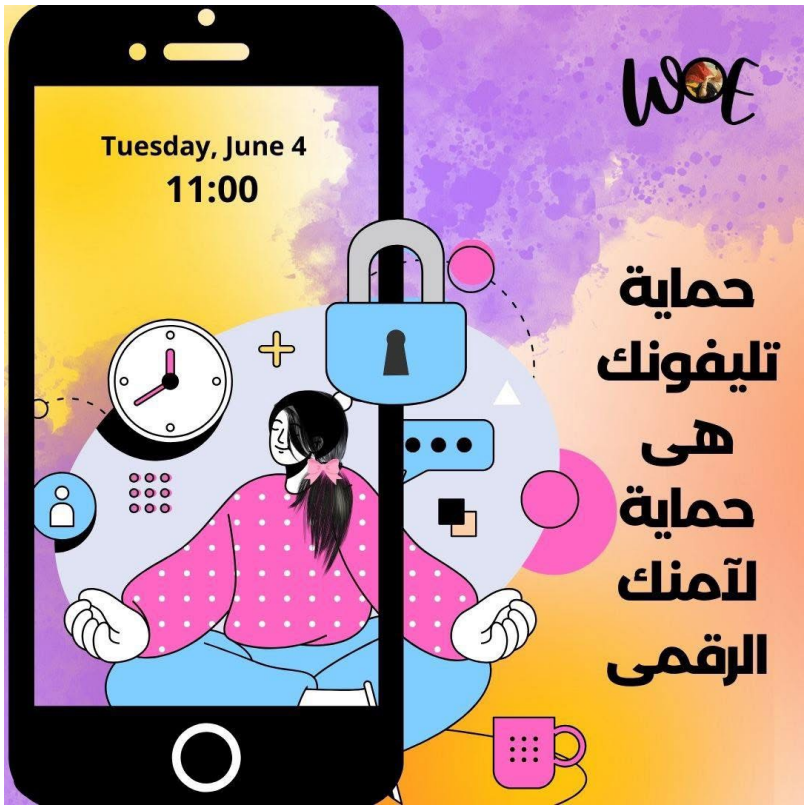
⭕ بلاش تستخدمى الكلمات الشائعة زى "iloveyou" ,"password", الخ.

⭕ بلاش تستخدمى التسلسل (زى: abcd1234) أو الحروف اللى ورا بعض على الكيبورد (زى qwerty).

⭕ غيرى كلمة السر باستمرار

⭕ متنسيش تكتبيها في مكان آمن بحيث تقدرى تلاقيها بسرعة وقت ما تحتاجى لها

تأمين شاشة قفل الموبايل Screen Lock



🔴 آمنتى تليفونك النهاردة ! حماية تليفونك هى حماية لخصوصيتك ولأمنك الرقمى

⭕ تعرفى ان اى ممكن اى حد يوصل لبيانات تليفونك لو معندكيش Screen Lock تأمين قفل لشاشة التليفون.

⭕ وبالرغم من أهميتها، اغلب الناس مش بتهتم انها تأمن شاشة قفل التليفون.

⭕ صحيح إن كتابة كلمة او رقم مرور كل مرة عاوزة تشوفى حاجة على التليفون مزعجة جدا، بس هى خطوة مهمة علشان تحافظى على خصوصية تليفونك، وعلى أمنك الرقمى

⭕ تليفونك ممكن يضيع، ممكن تنسيه فى التاكسى، او فى كافيه؛ وممكن مديرك فى الشغل يندهك وتسيبى التليفون على المكتب؛

⭕ لو معندكيش تأمين شاشة قفل التليفون، انتى بتدى بياناتك "هدية" لأى شخص عاوز يأذيكى، لأنه فى غمضة عين هيقدر يوصل لكل حاجة على تليفونك: ملفاتك الشخصية، صورك، حسابك على فيسبوك، وتطبيقات التسوق.

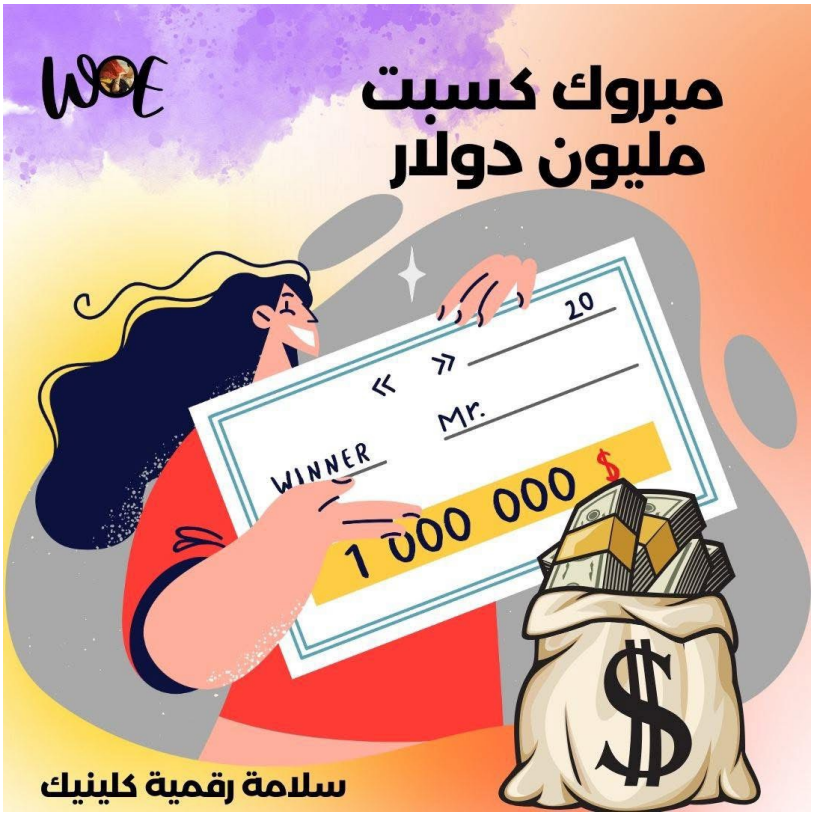
⭕ ولو تليفونك حافظ كلمات المرور بتاعتك، الهاكر او الشخص اللى عاوز يأذيكى هيقدر يدخل على أي موقع عندك، و يستخدم المعلومات الموجودة ضدك.

⭕ خطوات تأمين شاشة قفل التليفون بسيطة جدا ومش حتاخد منك خمس دقايق علشان تفعليها.

⭕افتحى تطبيق "الإعدادات" على تليفونك، وبعدين دوسى على "الأمان"، دوسى على قفل الشاشة واختارى طريقة القفل اللى تناسبك

⭕ اتبعى التعليمات على الشاشة

ازاى تحمى نفسك على الانترنت؟



🔴 اول قاعدة فى استخدام الانترنت هى انك متضغطيش على اى لينك يوصلك فى ايميل او مسيدج لانها ممكن تكون برامج ضارة وتعرض جهازك للخطر؛ وعلشان كده:

⭕ اوعى تعملى داونلود لملف وصلك فى ايميل انتى مش مستنياه.

⭕ مفيش حاجة اسمها حد بعت لكم ايميل يقول لكم انتم كسبتوا يانصيب واضغط على اللينك ده

مفيش حد حيكسب جايزة مالية بدون سبب. دى حاجات بتخليكى تلغى تفكيرك وتضغطى على اللينك.

⭕ اوعى تنزلى ملفات وصلتك فى ايميل او مسيدج فيها اخبار مغرية او حصرية

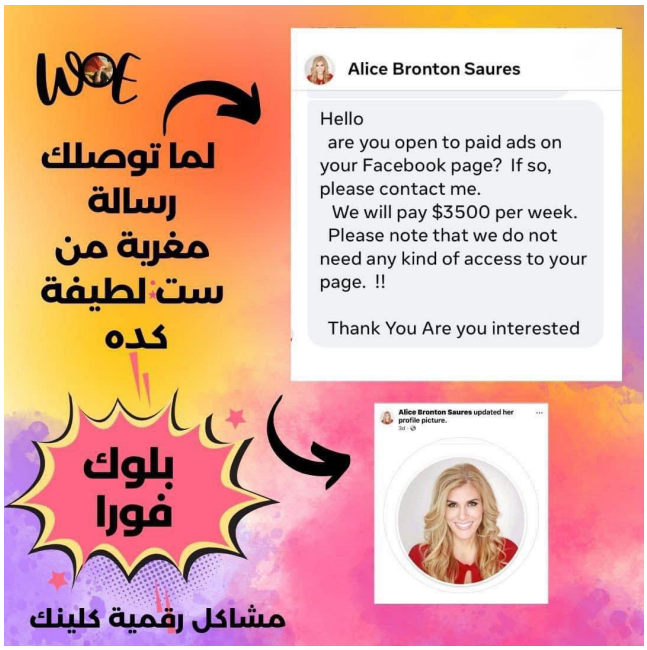
⭕ اوعى تردى على ايميلات او رسائل بتطلب كلمة السر بتاعتك.

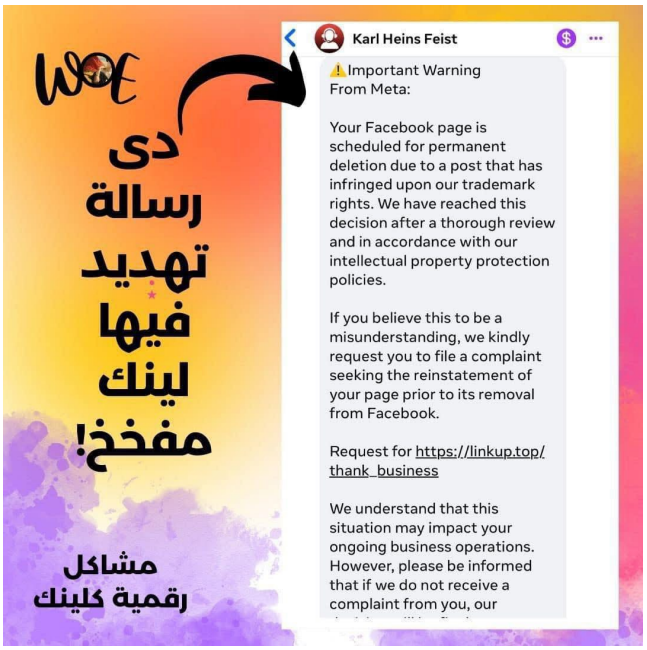
⭕ اوعى تنزلى اى تطبيق او سوفت وير او برنامج للكمبيوتر او التليفون من مواقع غير رسمية علشان مجانية.

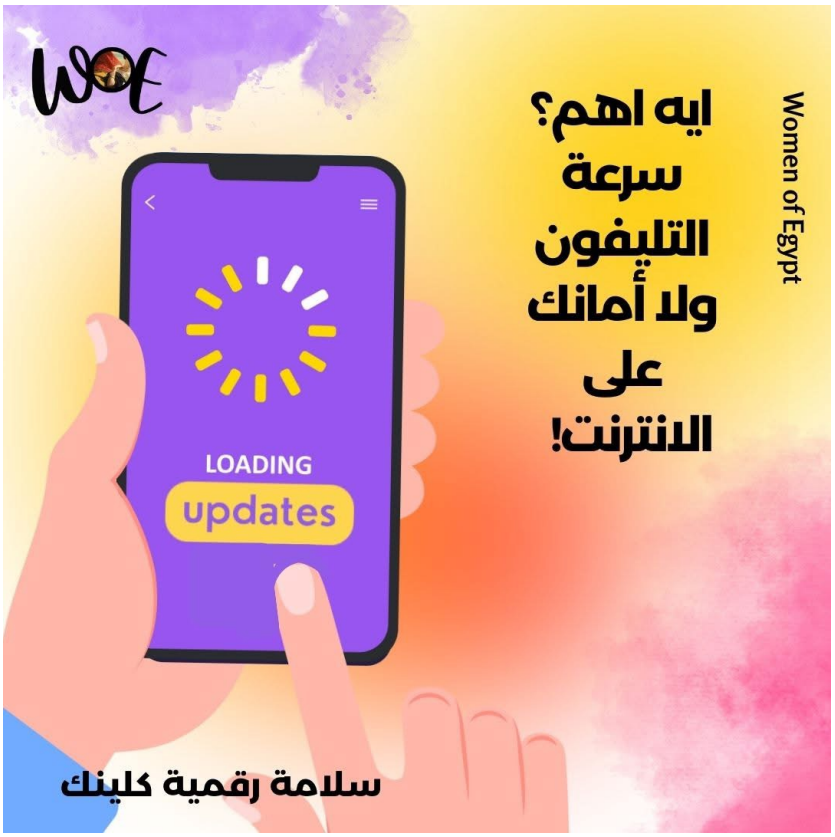
اى حاجة بتنزل من مواقع غير رسمية بيكون متحمل عليها برمجيات خبيثة.

⭕ حماية جهازك = حماية بياناتك = إنترنت اكثر أمان

أمثلة لرسائل بها لينكات مشبوهة







أهمية تحديث التليفون - Update

🔴 ناس كتير مش بتعمل تحديث "آبديت" لتليفوناتها لانها بتخاف انه:

⭕ حياخد مساحة من الجهاز

⭕ حيبطء سرعة التليفون

⭕ الأجهزة القديمة فعلا ممكن تبطء سرعتها شوية بس لو معملتيش تحديث "آبديت" انتى كده بتعرضى جهازك للخطر.

🔴 ايه اللى بيحصل لو معملناش "آبديت"؟

⭕ الشركات بتطلب "آبديت" لاجهزتها لما بتكتشف ثغرات ممكن تسمح لهاكر انه يخترق الجهاز.

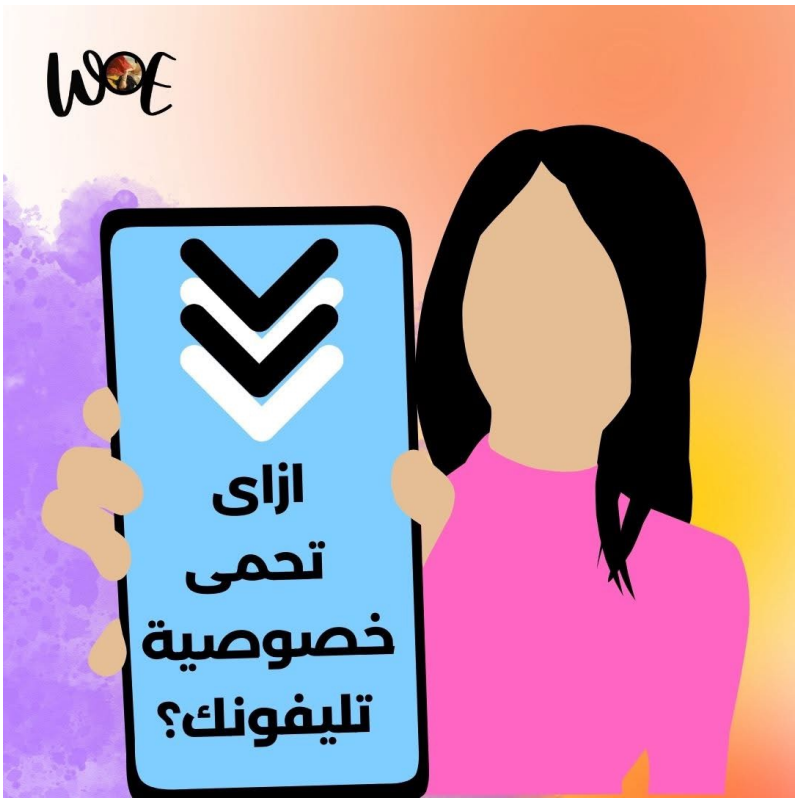
⭕ ناس كتير فاكرة ان التحديث "الآبديت" هو تغيير شكل بس، لكن الحقيقة ده بيقفل الثغرة الأمنية دى، و بيحمى الجهاز من الڤيروسات ومن محاولات اختراق.

⭕ لو مقفلناش الثغرة دى، اول حاجة بيعملها الهاكر انه يشوف مين معملش تحديث "آبديت" ويخترق جهازه

⭕ هو يعنى الهاكر حيسيب الكام بليون جهاز اللى فى العالم ويخترق جهازى أنا؟

⭕ ايوة ! انتى وكل حد تانى جهازه فى ثغره هدف الهاكرز.

إزاي تحمي خصوصية تليفونك؟



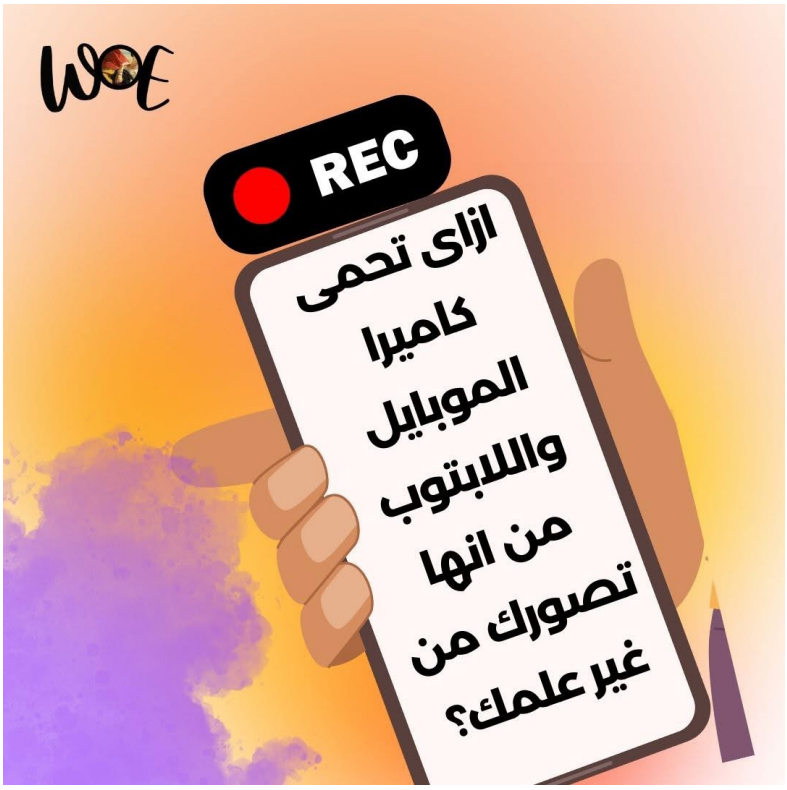
آمنتى تليفونك النهاردة! | إذا حد قدر يوصل لبيانات تليفونك أو لقى طريقة يخترق جهازك، ممكن يستخدم المعلومات اللي على التليفون ضدك. علشان كده، مهم إنك تحمي تليفونك، ودى خطوات بسيطة حتساعدك على كده:

⭕ متنزليش تطبيقات غير من الآب ستور (متجر التطبيقات)؛ وده لأن الآب ستور بيوفر بعض الحماية ضد البرامج الضارة. وكمان تليفونك بيفحص بانتظام البرامج اللى نزلتيها من الآب ستور عشان يتأكد إنها آمنة.

⭕ لما تنزلى تطبيق جديد، انتى تقدرى تتحكمى فى البيانات اللى بيطلب التطبيق انه يوصل لها، زى الملفات و الكاميرا، وموقعك الجغرافى.

⭕ ارفضى التطبيق اللى عاوز يوصل لأى معلومات شخصية عنك، او لقائمة معارفك (الكونتاكتس)؛ وابحثي على تطبيق مشابه مش بيطلب البيانات دى.

ازاى تحمى كاميرا الموبايل واللابتوب من انها تصورك من غير ما تعرفى؟



⭕ بعض التطبيقات بتشغل كاميرا الموبايل واللاب توب من غير ما تعرفى؛ وعلشان كده مهم جدا انك تحمى كاميرا الموبايل او اللاب توب علشان متشتغلش وانتى مش واخدة بالك.

⭕ دى شوية خطوات سهلة حتساعدك تحمى كاميرتك واللى بدورها حتحمى خصوصيتك، وتحميكى من التعرض لابتزاز الكترونى لو الصور دى وقعت فى ايد شخص مش أمين.

⭕ إبعد عن التطبيقات اللي مصدرها مش معروف، ونزل التطبيقات بس من Google Play أو App Store.

⭕ راجعى التطبيقات على تليفونك، وشوفى التطبيقات اللى ممكن توصل للكاميرا ، واقفليها لو مش محتاجة تستخدمى الكاميرا

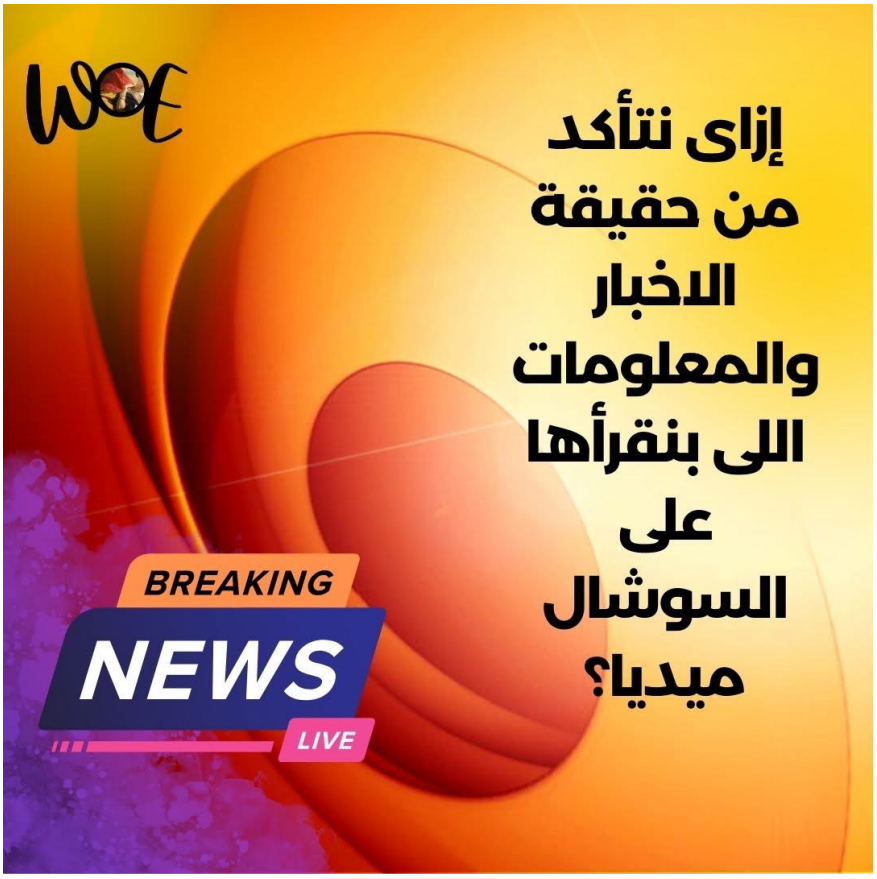
⭕ كاميرات التليفون واللاب توب ممكن تشتغل عن بعد. تأكدى دايما انك تقفلي الأجهزة دى لو مش بتستخدميها

⭕ تأكدى دايما ان كاميرا اللاب توب متغطية. لو الكاميرا ملهاش غطاء، ممكن تغطيها بستيكر

⭕ متديش أذن لكل تطبيق بتنزليه انه يوصل للكاميرا. فى تطبيقات مش بتحتاج الكاميرا

⭕ اعلمى تحديث لبرامج مكافحة الفيروسات اول بأول، ودايما تأكدى ان التطبيقات مصدرها موثوق فيه.

ازاى نتأكد من صحة المعلومات اللى بنقراها على الإنترنت؟



⭕ الإنترنت والسوشال ميديا اصبحوا مصدر للأخبار والمعلومات لناس كتيرة اوى.

⭕ هل بتفكروا قبل ما تشييروا لو الاخبار دى صحيحة ولا دى اشاعات؟ وايه الضرر اللى ممكن تحصل لو نشرنا معلومات مش صحيحة؟

⭕ بس أولا لازم نفرق بين المعلومات الغلط والمعلومات المضللة.

⭕ المعلومات الغلط هى اللى بننشرها من غير ما نتأكد من مصدرها أو صحتها، والمعلومات دى بالرغم من انها ممكن تكون غير منطقية، لكن ، بسبب قلة الوعى، الناس بتنشرها من غير نية للايذاء

⭕ المعلومات المضللة بتتكتب وتتنشر مخصوص علشان تضر الناس، وبيتم اعادة تداولها (تشييرها) من غير ما بنتأكد من صحتها.

⭕ صانعى محتوى المعلومات المضللة بيستخدموا الانترنت والسوشال ميديا علشان توصل والمعلومات المضللة لأكبر عدد من الجمهور.

⭕ علشان كده من المهم قبل ما نصدق أي حاجة بنقراها ونشيرها، وخصوصًا لو كانت الأخبار أو المعلومات مش منطقية، لازم نتأكد من:

⭕ المصدر: مين اللي كتب الخبر؟

⭕ مين صاحب الحساب (الاكاونت) اللى نزل عليه الخبر؟

⭕ هل الاسم اللى مكتوب على الاكاونت حقيقي ولا اسم وهمى؟

⭕ هل الشخص صاحب الحساب ده له اصحاب ومتابعين كتير ولا لا؟

⭕ التاريخ: الحساب أو الموقع اللى نزل عليه الخبر ده جديد ولا لا؟

⭕ الموقع: هل موثوق فيه وله مصداقية؟ وهل محريرين الموقع ده أشخاص حقيقية ولا لا؟

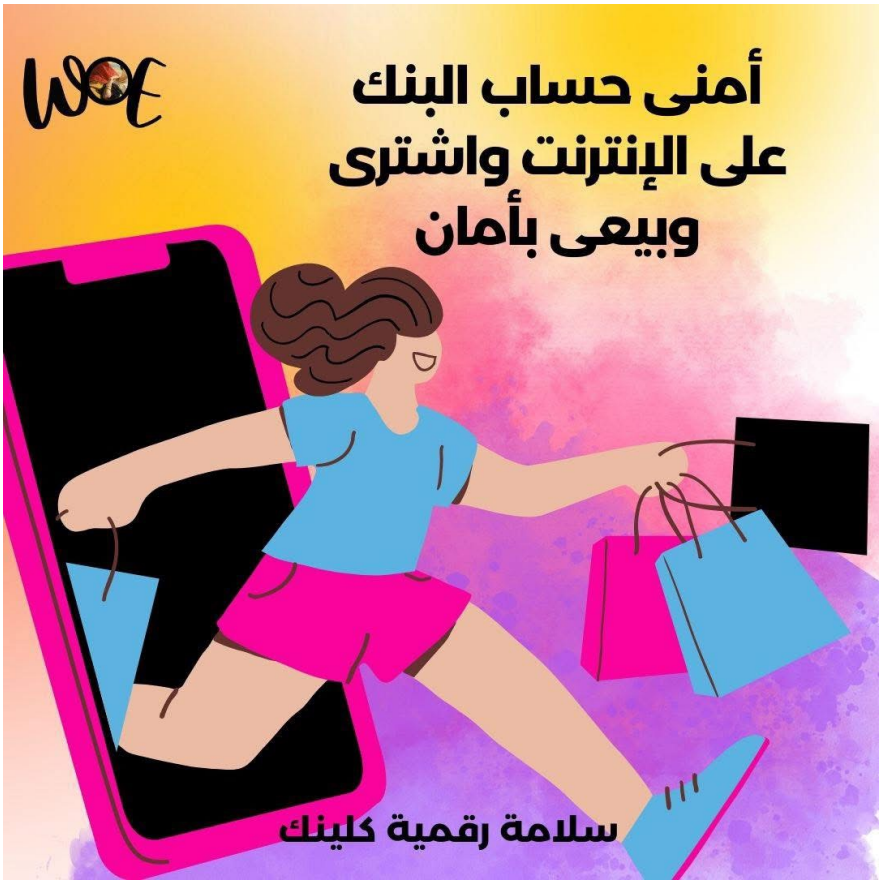
⭕ الدافع: ليه ظهر المحتوى ده فى التوقيت ده؟

⭕ هل المعلومات والأخبار دى منطقية ولا لا؟

⭕ هل الخبر ده نزل على اكتر من موقع محترم وموثوق فيه، ولا لا؟

الحاجات دي بتساعدنا نتأكد إن المعلومات اللى بنقراها صحيحة قبل ما نصدقها ونشييرها.

الشراء بأمان علي الإنترنت



🔴 معظمنا بيستخدم الإنترنت علشان نشتري و نبيع و ندفع فواتير واشتراكات أونلاين، الحاجات دي كلها بتعرض حساباتنا البنكية للخطر.

الخطوات البسيطة دى حتساعدك تحمى حسابك البنكى وتقللي فرص تعرضك للاختراقات والسرقات.

⭕ مش حنفكرك بأهمية استخدم كلمات مرور طويلة ومعقدة وفيها حروف كبيرة وصغيرة وأرقام ورموز.

وكمان بلاش تستخدمى نفس كلمة المرور لأكتر من حساب.

⭕ المصادقة الثنائية او التحقيق بخطوتين، ودى معناها انك تأمنى حسابك زيادة بإضافة رقم تليفونك على الحساب.

⭕ تابعى حساب البنك بانتظام عشان تقدرى تكتشف بسرعة أي نشاط غريب.

⭕ متفتحيش حساب البنك وانتى بره البيت من شبكة واى فاى عامة فى محل او كافيه او نادى.

⭕ اعملى تحديث لتليفونك باستمرار علشان تتأكدى ان التطبيقات اللى بتستخدميها مفيهاش ثغرات ممكن الهاكر يخترق التليفون منها.

⭕ استخدمى التطبيق الرسمي للبنك بتاعك مش تطبيقات طرف تالت. التطبيقات الرسمية بتكون أكتر أمان وبتضمن حماية بياناتك.

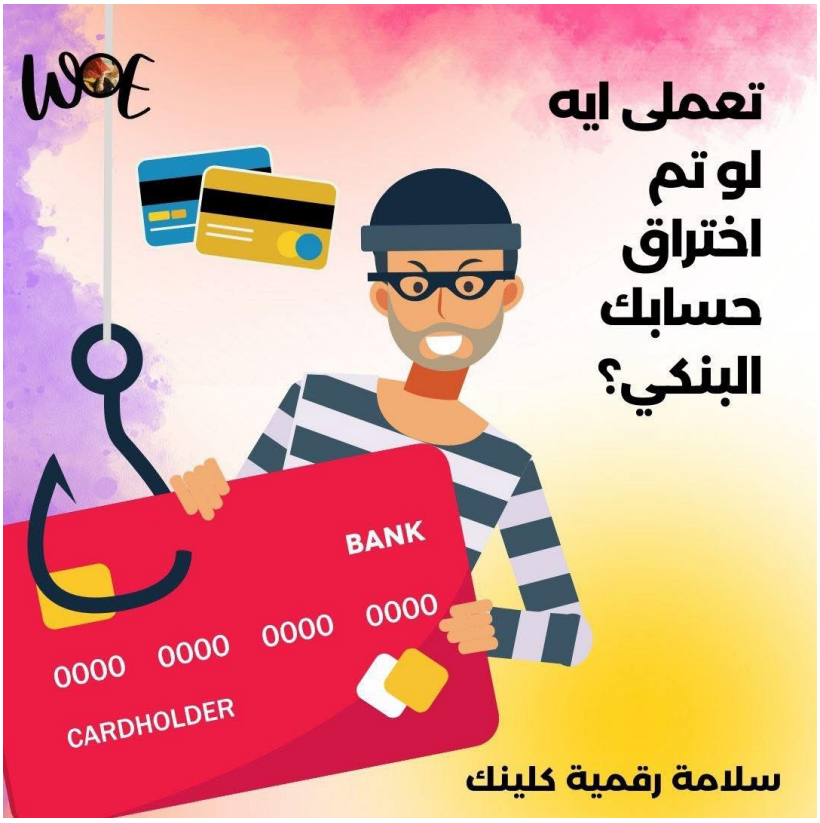
⭕ وبرضه مش حنفكرك بلاش تفتحى اى لينكات بتوصلك فى رسائل

⭕ اوعى تبعتى معلومات شخصية أو بنكية لأي رسائل غير معروفة أو مشبوهة. البنوك عمرها ما هتطلب معلومات حساسة بالطريقة دي.

⭕ نزلي برامج مكافحة الفيروسات وبرامج الحماية على جهازك عشان تحمي نفسك من الفيروسات والبرامج الضارة.

🔴 طيب تعملى ايه لو أتعرض حساب البنك للاختراق؟

تعملي ايه لو تم إختراق حسابك البنكي؟



🔴 معظمنا بيستخدم الإنترنت علشان نشتري و نبيع و ندفع فواتير واشتراكات أونلاين، الحاجات دي كلها بتعرض حساباتنا البنكية للخطر.

طيب تعملى ايه لو حصل اختراق لحسابك البنكى؟

⭕ أول حاجة تعمليها هى انك تتصلى بالبنك فورا وتبلغيهم ايه اللى حصل وتطلبى تجميد الحساب وتلغى الكارت علشان تمنعى اى معاملات تانية تتم بإستخدامه.

⭕ لو لسه عندك إمكانية دخول حسابك، غير كلمة المرور بتاعتك فورًا واختار كلمة مرور جديدة وقوية.

⭕ لو مش مفعلة خاصية التحقق بخطوتين، فعليها دلوقتي عشان تضيف طبقة أمان زيادة لحسابك.

⭕ راجعى حسابك البنكي وشوف المعاملات الأخيرة عشان تقدرى تحدد المعاملات اللي انت ما عملتهاش، وتبلغى بيها البنك.

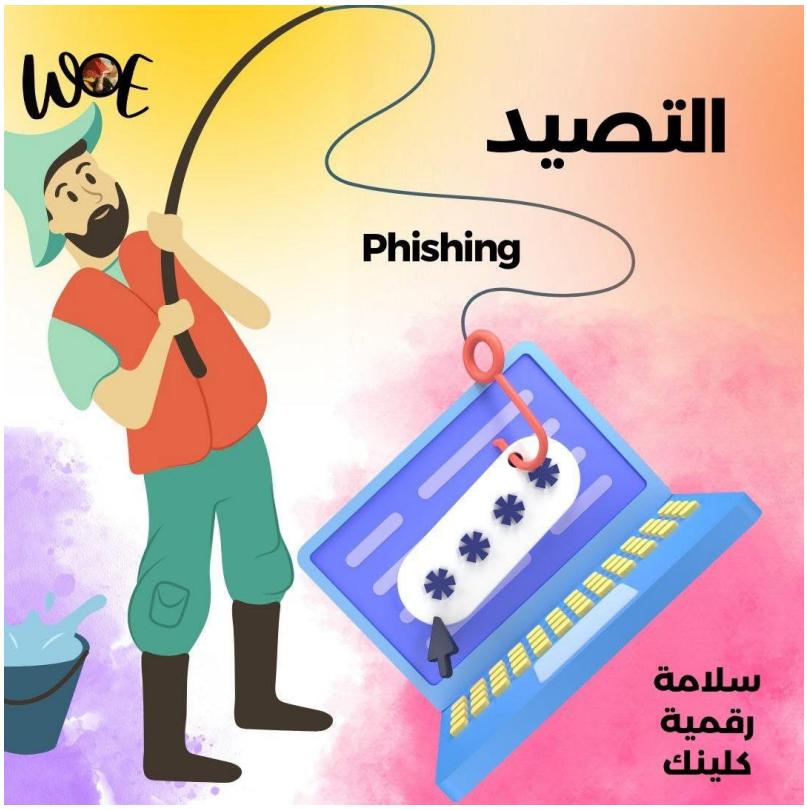
⭕ شغلي برنامج مكافحة الفيروسات وافحص جهازك بالكامل علشان تتأكدى ان مفيش فيروسات أو برامج ضارة ممكن تكون هى السبب في الاختراق

⭕ تابعى حسابك البنكي بشكل منتظم في الفترة الجاية عشان تقدرى تكتشفى أي نشاط غريب بسرعة وتبلغ عنه.

⭕ لو بتستخدمى نفس كلمة المرور في حسابات تانية، غيرها فورًا عشان تحمى باقى الحسابات من الاختراق.

🔴 الإجراءات دي هتساعدك تقللى الخساير اللي ممكن تحصل نتيجة اختراق حسابك البنكي، وكمان وحتحمى حسابك البنكى وتقللي فرص تعرضك للاختراقات والسرقة فى المستقبل

تعريف التصيد



التصيد او الفيشينج أصبح من أكتر الحيل اللي بيستخدمها الهاكرز لإختراق الحسابات، و بيستخدموا تقنية عالية جدا أحيانا بيكون من الصعب كشفها.

⭕ ازاي بيتم اختراق الحسابات بـ الـ فيشينج؟

⭕ بيوصلك ايميل من شركة مشهورة أو بنك، بيحذرك ان حسابك حيتقفل، او إنك كسبت خدمة أو فلوس، أو ان عليك فلوس لهم، أو حجة تانية يحاولوا فيها انهم يوجهوكي انك تضغطي علي رابط موجود في الإيميل.

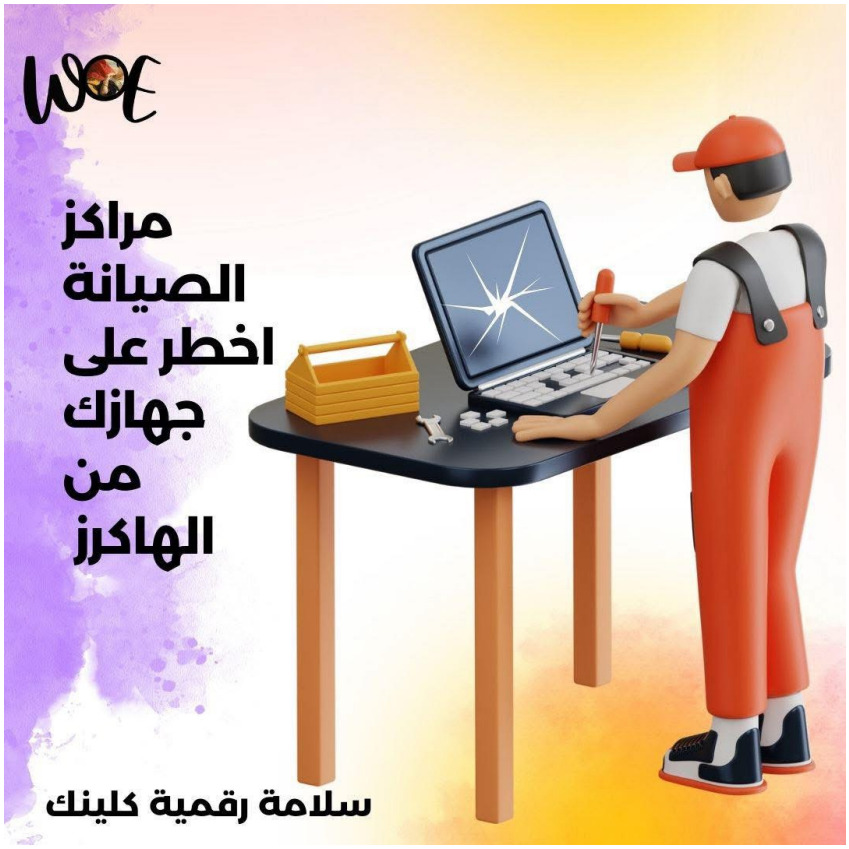
⭕ وفي الرابط ده بيتطلب منك انك تدخلي الباسوورد او رقم الكريديت كارد. الروابط دي بتوصل جهازك لمواقع بيقدروا من خلالها سرقة بياناتك.

⭕ علشان تحمي حسابك من الإختراق، بلاش تضغطي علي الروابط في رسائل البريد الإلكتروني اللي بتوصل من أشخاص مجهولين

⭕ وفي حالة لو وصلك لينك مش مستنياه في ايميل من حد تعرفيه، مش حتخسرى حاجة لو اتأكدتى بنفسك من صاحب الايميل انه هو فعلا اللي بعته

لانه هو نفسه ربما يكون كمان حسابه تم اختراقه، والهاكرز بيبعتوا ايميلات لأصحابه علشان يخترقوا حساباتهم هم كمان

كيف تتخلصي من جهازك القديم؟



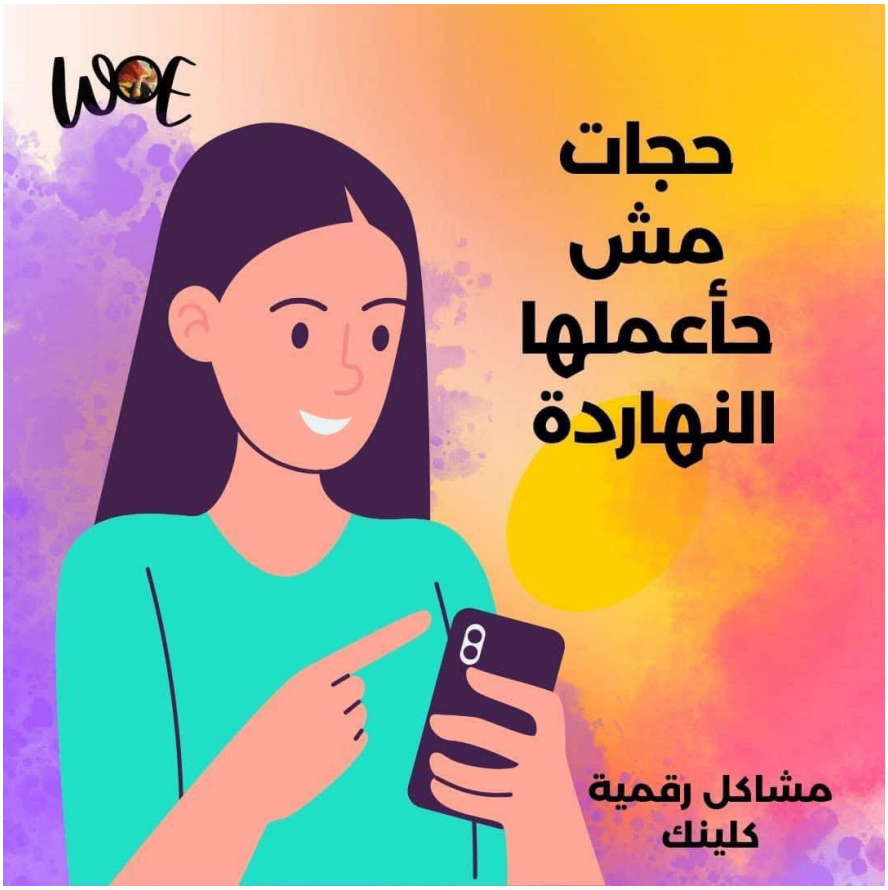
بياناتك مش بتتسرق بس لو حد اخترق جهازك، دى ممكن كمان تتسرق من جهاز اشتراه حد منك أو وديتيه لمركز صيانة علشان يتصلح!

علشان كده، مهم جدا قبل ما تبيعي أو تتخلصي من جهاز كمبيوتر قديم، أو موبايل، أو أي جهاز تاني مخزن عليه بياناتك، تتأكدي إنك مسحتي كل بياناتك وأي معلومات شخصية أو سرية عليه، وتمسحيها بشكل نهائي وترجعيه لإعداداته الأصلية.

يعني الجهاز يروح لمركز الصيانة أو للمشتري الجديد وهو نضيف تماما.

وكمان، افضل طريقة علشان تتخلصي من فلاشات أو سيديهات أو أي أجهزة تخزين تانية، هو انك تكسريها ... تحطميها ... تدغدغها ... قبل ما ترميها.

كيف تحمي حسابك علي فيس بوك من الإختراق



🔴 علشان تحمى اكاونت فيس بوك من الاختراق :

⭕ متضغطيش على اى لينك يوصلك فى الانبوكس، مهما كان عنوانه مغرى انك تفتحيه، وحتى لو اللى بعته اعز أصحابك!

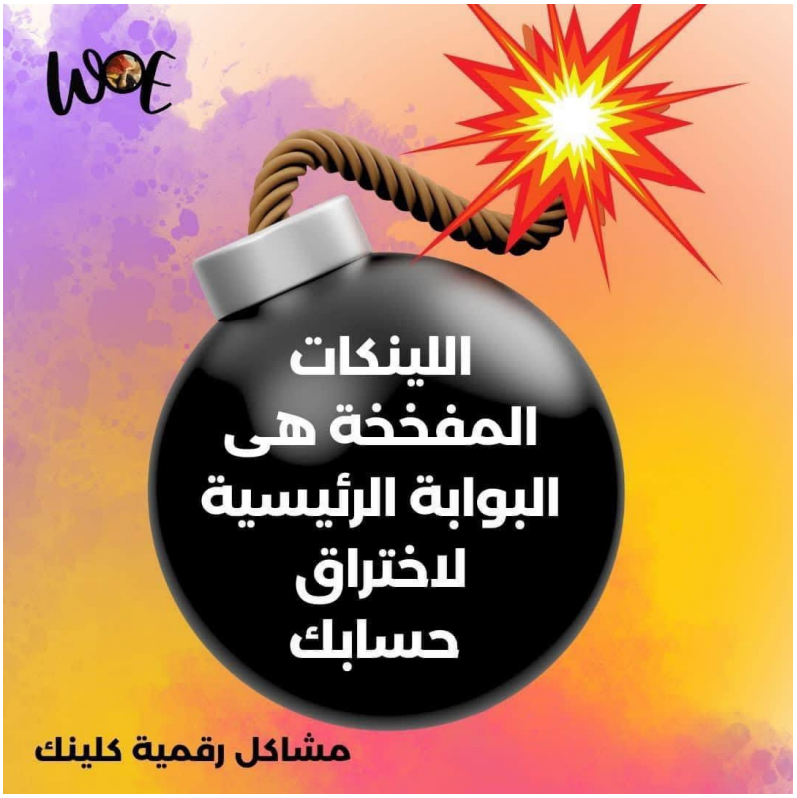
⭕ مش حتفتحيه مش علشان مفيش ثقة فى أصحابك، لكن علشان مفيش ثقة فى اللينك اللى وصلك! ممكن

حساب اعز أصحابك ممكن بكون تم اختراقه وانتى مش عارفة، واللينك بعته الهاكر.

⭕ لو اللينك من فيس بوك بيكون مكتوب عليه فيس بوك، وبيكون باين معمول له شير من اى صفحة.لكن اللينكات اللى فيها حروف وأرقام وعلامات، دى كلها خطر جدا.

🔴 طيب ازاى جهازى بيتعرض لاختراق بسبب اللينكات دى؟

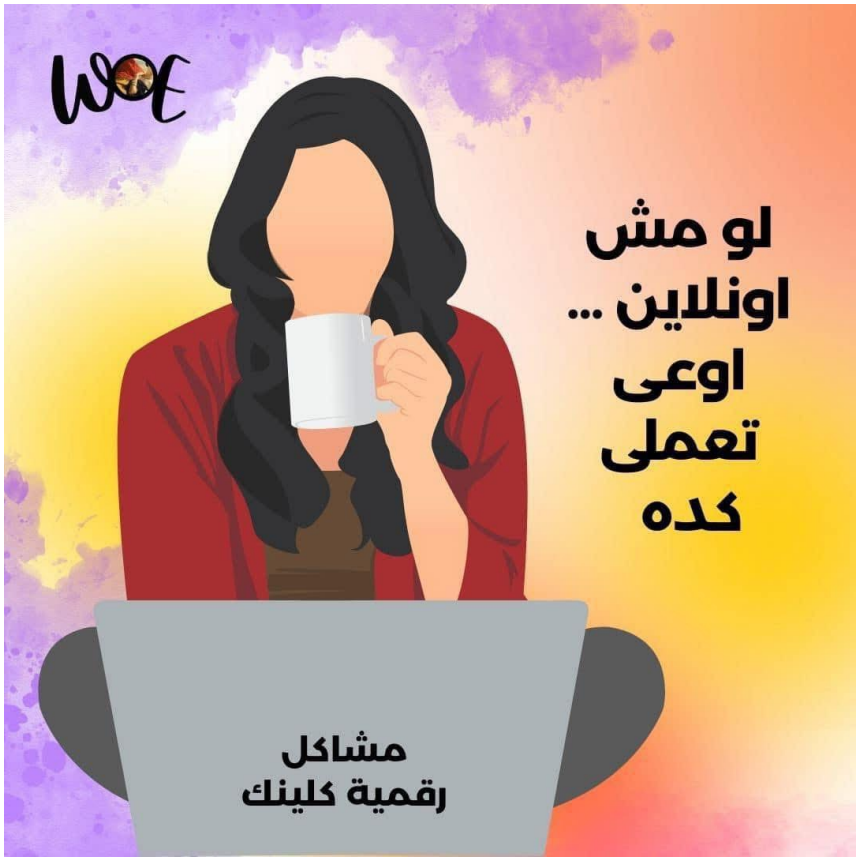
⭕ اللينكات الغريبة اللى بتوصل فى الانبوكس دى بيبعتها الهاكر، واول ما تدوسي عليها حسابك بيتم اختراقه. والحساب بيقع فى ايده، ويستولى عليه؛ و صورك وفيديوهاتك وقائمة اصحابك وللرسايل اللى بتبعتيها فى الانبوكس.



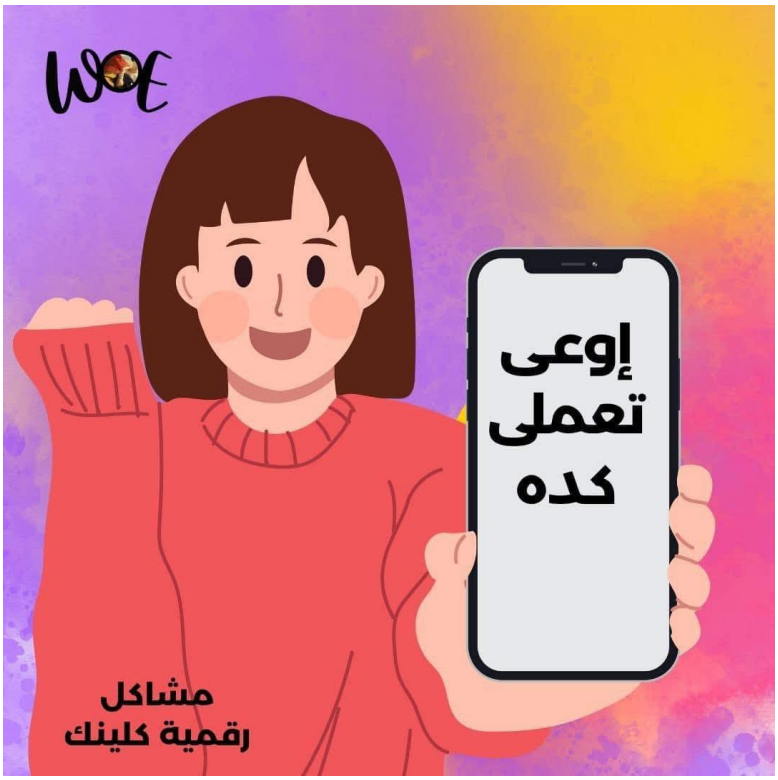
اوعى تدوسى على اى لينكات بتوصلك فى ايميلات او مسيدحيز مهما كانت مغرية او اخبارها حصرية او فيها جايزة بمليون جنية. كل اللينكات دى مفخخة .. الغرض منها هو اختراق حسابك.

نصائح للحماية اون لاين

!!لو انتى مش اونلاين اوعى تعملى كده :



- تسليم أجهزتك لاى شخص
- متستخدميش كومبيوتر من اى مكان (Internet cafe)
- تسيبى الكمبيوتر دون مراقبة أو بدون lock
- متستخدميش USB وانتى مش عارفه عليها فيروسات ولا لا

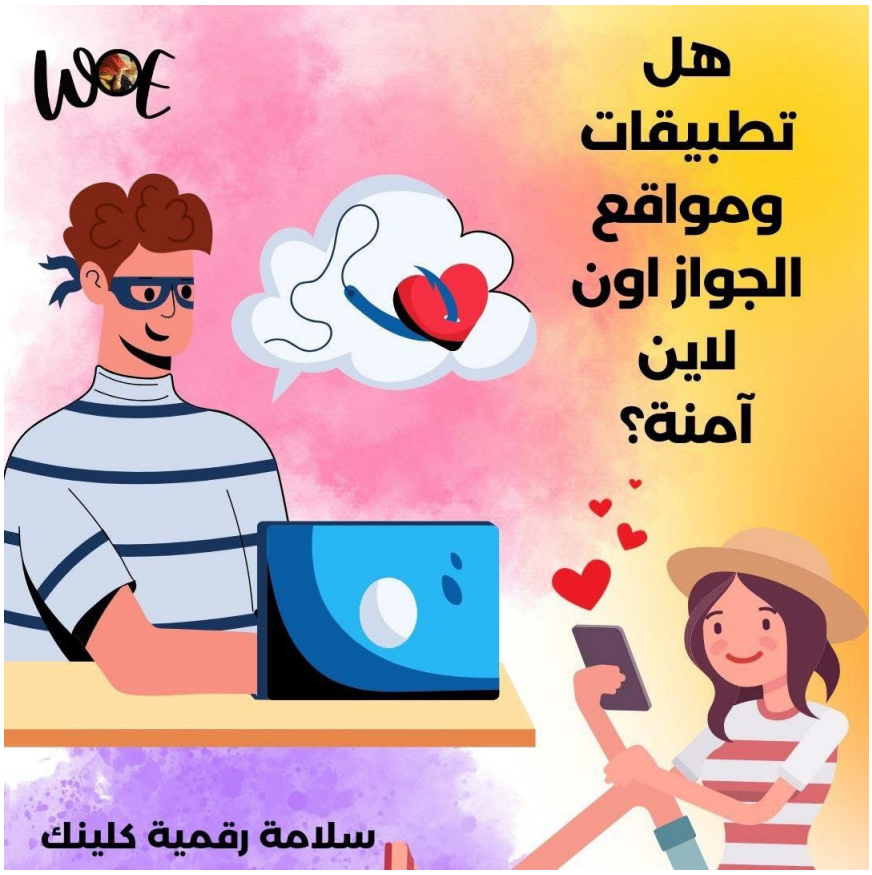


!!

اوعى تعملى كده :

- تبعتى معلومات شخصية أو ماليه خاصه بيكى
- اوعى تنزلى ملف من الايميل انتى مش مستنياه
- اوعى تقبلى رسايل من الايميل من برامج مبروك كسبتى
- اوعى تنزلى ملفات مجهولة (حصرى صور الفنانة ...)
- تنزيل برامج من مواقع غير رسمية
- اوعى تبعتى او تردى على أيميل تطلب كلمه السر الخاصة بيكى

هل تطبيقات ومواقع الجواز اون لاين آمنة؟



⭕ الإنترنت غير بشكل كبير طريقة الجواز التقليدية، وخصوصا بعد ما ابتدت تنتشر مواقع وتطبيقات التعارف والجواز أونلاين، واللى بنات وشباب كتير فعلا استخدموهم علشان يلاقوا شريك حياتهم

⭕ المواقع والتطبيقات دى بتوفر وقت وبتدي خيارات كتير، وده اللي بيدور عليه الشباب دلوقتى. لكن المواقع دى كمان بتعرض مستخدميها للجرائم الالكترونية والنصب والاحتيال.

⭕ هل فكرتي في المخاطر اللي ممكن تتعرضى لها لو استخدمتي المواقع دي من غير ما تعرفي أساسيات الأمان الرقمي والنفسي؟

🔴 من اكتر المخاطر اللي ممكن تقابليها على مواقع الزواج أونلاين:

⭕ الابتزاز الإلكتروني

⭕التشهير

⭕انتحال الشخصية

⭕ الاحتيال الإلكتروني: النصابين بيعملوا حسابات مزيفة على مواقع الجواز اون لاين وبيصوروا نفسهم انهم في مجالات ومناصب مرموقة. ويكسبوا ثقة السيدات من خلال رسائل أو تليفونات.

⭕ علشان كده المواقع دي ممكن تكون خطيرة جدًا ، لأن التعارف من خلالها ممكن يوصل للابتزاز الجنسي أو المالي أو حتى لجرائم حقيقية، لان النصابين يستغلوا رغبة الضحية فى الجواز والاستقرار ويستخدم المواقع دى عشان يوقعوا بها.

🔴
ومن اجل سلامتك وانتى بتستخدمى المواقع دى:

⭕ حافظى على خصوصيتك والمعلومات الشخصية عنك تكون في أضيق الحدود.

⭕ متتواصليش مع ناس مجهولة.

⭕ ما تضغطيش على أي لينكات يبعتهالك الطرف التانى، ولا اغنية رومانسية ولا إعلان ولا اى حاجةً تانية.

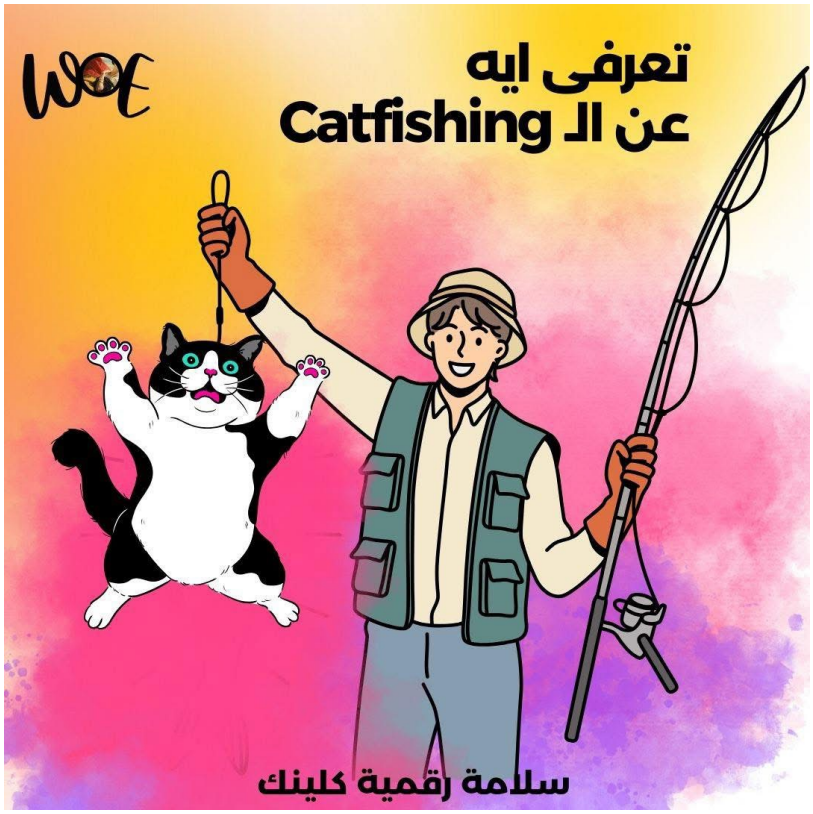
⭕ ما تبعتيش فلوس أو تقدمي مساعدة مالية لحد اتعرفتى عليه اون لاين.

⭕ وافتكرى دائماً أن اى حاجة قلتيها او بعتيها اون لاين ممكن تستخدم ضدك. ما تبعتيش صور او فيديوهات شخصية ليكى.

ايه هو الكات فيشين Catfishing وازاي تحمي نفسك منه؟

مصطلح Catfishing بالإنجليزي ملهوش علاقة بصيد القطط. الكات فيشينج معناها انتحال شخصية مزيفة اون لاين، علي صفحات التواصل الإجتماعي.

⭕ النصابين بينتحلوا شخصية مزيفة وبيستخدموها للنصب والاحتيال



⭕ المجرمين بيشتركوا باسماء وصور مزيفة علي مواقع التعارف والدردشة وصفحات التواصل الإجتماعي، وتطبيقات الجواز اون لاين، ويعملوا علاقات عاطفية وهمية، ويوعدوا الضحية بالجواز، وبعد ما بيعرفوا اسرارهم وبياخدوا صورهم الخاصة بيبتدوا يبتزوهم

⭕ الكات فيشينج هو نوع من أنوا ع العنف الإلكتروني، وبالرغم من ان مفيش قانون ضد انتحال شخصية مزيفة أون لاين، ولكن الـ Catfishing في أغلب الأحيان هو الخطوة اللي بتسبق الإبتزاز الجنسي، واللي هو جريمة بيعاقب عليها القانون.

🔴 دي علامات إن الشخص اللي بتتواصلي معاه شخصية مزيفة:

⭕ معندهوش أصدقاء او متابعين كتير علي حسابه

⭕ بيتهرب من أي إتصال تليفون أو فيديو

⭕ صورة البروفايل رسمية ومش بيغيرها ، ومش حتلاقى له صور سيلفى

⭕ بيرفض المقابلة وغالبا الحجة انه بيشتغل بره

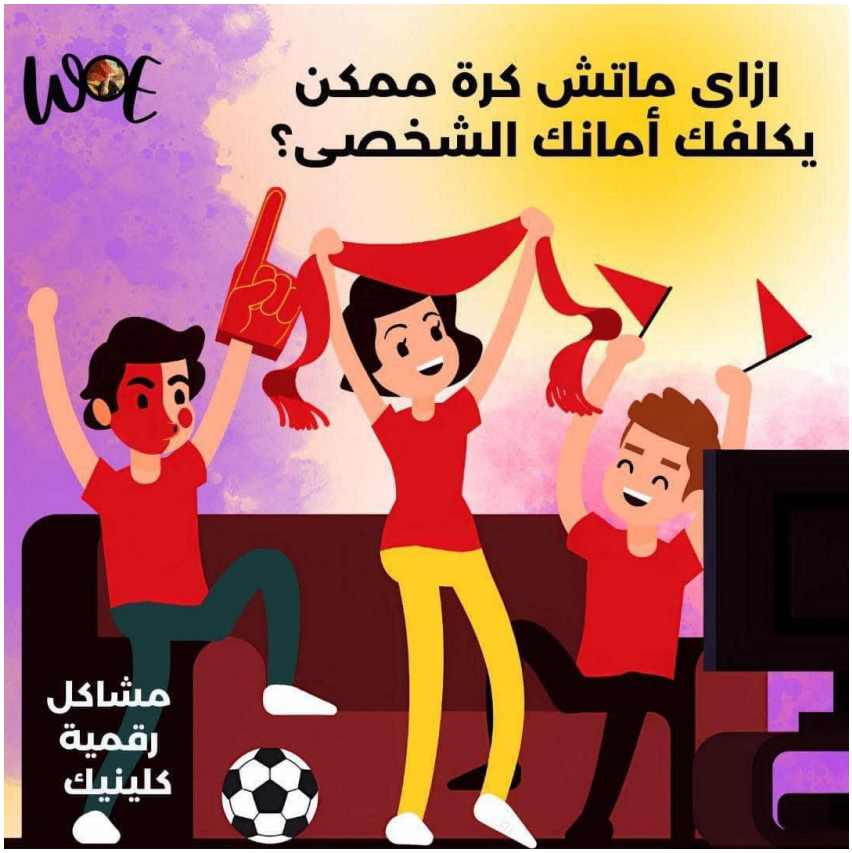
⭕ بيعترف بإعجابه أو حبه لكي بسرعة جدا

⭕ حكاياته ملخبطة

⭕ بيطلب منك فلوس

🔴 لو في حد من أصدقاءك علي صفحات التواصل الإجتماعي او غرف الدردشة بينطبق عليه المواصفات دي، أعملي له بلوك علي طول. ده شخصية مزيفة غرضه ايذائك، بس منتظر الفرصة المناسبة.

ازاى ماتش كرة ممكن يكلفك أمانك الشخصي؟



- فى تطبيقات كتيرة بننزلها علشان بتفتح الماتشات المشفرة. عمرك سألتى نفسك ليه التطبيقات دى مجانية؟

- الاجابة سهلة جدا، لانها كلها لينكات مفخخة

- الهاكرز بينشطوا جدا وقت الماتشات، واول ما بتدوسى على لينك علشان تفتحى الماتش، حسابك بيتم اختراقه!

- الماتش مهما كان مهم مش اهم من أمانكم الشخصى