FİLİSTİN İLETİŞİMCİLER VE MEDYA DERNEĞİ
الجمعية الفلسطينية للإعلام

2021/01/13

مخرجات الندوة التخصصية حول:

الخصوصية والأمان على منصات التواصل الاجتماعي

-الواتس آب نموذجاً-

المتحدثون في الندوة:

م. أشرف مشتهى	م. أسامة صيام	أ. خالد صافي
المختص بالتقنية وأمن المعلومات	المختص بالأمن السيبراني	المختص في التسويق الرقمي

أدار الندوة:

الصحفي: محمد أبو طاقية

إعداد وتنفيذ:

الجمعية الفلسطينية للإعلام – فيميد

ندوة "الخصوصية والأمان على منصات التواصل الاجتماعي – الواتس آب نموذجا"

بعد الجدل الكبير الذي أثير حول التحديثات الأخيرة المتعلقة بموضوع الخصوصية والأمان لتطبيق (واتس آب) المستخدم والمتداول بشكل واسع، والذي يضم الكثير من المجموعات الحوارية وغيرها.. قامت **الجمعية الفلسطينية للإعلام – فيميد** بعقد ندوة إلكترونية عبر تطبيق "ZOOM" تحت عنوان: "الخصوصية والأمان على منصات التواصل الاجتماعي – واتس آب نموذجا"، وذلك يوم الأربعاء الموافق ٢٠٢١/٠١/١٣ م حيث استمرت الندوة لمدة ساعتين تم بثها مباشرة عبر وكالة شهاب.

افتتح اللقاء بكلمة ترحيبية من أ. **إبراهيم المدهون** (المدير التنفيذي لجمعية فيميد)، حيث رحب بالحضور وشكر من قدم مساهمة ورقية منهم، وأكد أن **فيميد** هي بيت لكل الإعلاميين الفلسطينيين في تركيا حيث مقرها في إسطنبول، وتهدف لنقل الرؤية الفلسطينية للمجتمع التركي.. وأوضح أن هذه الندوة هي انطلاق لمجموعة من الندوات التي تناقش موضوع المحتوى الإعلامي الفلسطيني، وتبحث عن رؤية تفيد في الواقع الفلسطيني والإعلام الرقمي ومنصات التواصل الاجتماعي، وقد عبر عن أهمية هذه الندوة وتميزها بحضور ثلة من المختصين في هذا المجال، حيث رحب بالإخوة المتحدثين وهم: م. أشرف مشتهى، وم. أسامة صيام ، وأ. خالد صافي..

تحدث **م. أشرف مشتهى** -المختص بالتقنية وأمن المعلومات- حول شروط الخصوصية والأمان في برنامج (واتس آب) مقارنة في البرامج المنافسة والبديلة..

فيما تحدث **م. أسامة صيام** -المختص في الأمن السيبراني- حول التقييم التقني لمستوى الخصوصية والأمان لمستخدمي منصات التواصل الاجتماعي، ومقترحات التعامل الأمثل معها..

وتحدث **أ. خالد صافي** -المختص في التوسيق الرقمي- حول خصوصية المنظمات الفلسطينية في التعامل مع مجموعات (الواتس آب) والبرامج البديلة، بين المحاذير الأمنية وتعزيز التواصل والتثقيف الداخلي..

وفي ختام اللقاء تم فتح المجال للأسئلة والاستفسارات من جميع المشاركين والتعقيب والإجابة عليها، وكانت هناك مداخلة خاصة لـ **أ. إياد القرا** -رئيس المركز الشبابي الإعلامي بغزة- تحدث فيها عن نية مركزهم إطلاق أداة تُستخدم عبر الهواتف المحمولة و تطبيق آخر عبر متصفح كروم، كخطوات تقنية وعملية لمواجهة الحرب المفتوحة على المحتوى الفلسطيني في مواقع الإعلام الاجتماعي خاصة الفيس بوك.

وفي ختام اللقاء عبر **أ. محمد أبو طاقية** والذي أدار هذا اللقاء عن شكره لجميع الضيوف والمشاركين في هذه الندوة، على أمل اللقاء بالجميع في ندوات وورشات **فيميد** القادمة.

مداخلة م. أشرف مشتهى المختص بالتقنية في أمن المعلومات:

- لا يوجد خصوصية تامة أو أمان على مواقع التواصل في ظل هذا التطور التكنولوجي.
- الهدف الأساسي من الخصوصية والأمان هو تأمين خصوصية البيانات بين المتصلين، ويكون هذا المحتوى مشفر بخوارزميات معينة من ناحية فنية.
- واتس اب يستخدم تشفيرا يعتبر عاليا في المحادثات، ولا يطلع نظريا على المحادثات والبيانات بين المتصلين.
- الشركات المالكة لهذه المنصات ومنها واتس اب تجمع معلومات وبيانات كثيرة جدا حول المستخدمين دون الاطلاع على المحادثات، وهذا موجود مسبقا عند واتس اب.
- واتس اب لم يكن يشارك هذه المعلومات وفقا لسياستهم المنشورة، وحاليا سيقوم بمشاركة البيانات والمعلومات مع شركة فيس بوك، التي تستخدم وتبيع هذه البيانات مع الشركات الإعلامية والتجارية ولشؤون أخرى إن رأت ذلك.
- من تاريخ ٨فبراير ٢٠٢١ م سيكون المستخدم مجبرا على الموافقة على سياسة مشاركة المعلومات هذه وكل ما يتعلق بها، وإلا فإنه سيضطر لمغادرة واتساب مجبرا إن لم يوافق على ذلك.
- جميع التطبيقات تطلب نفس الأذونات من المستخدم تقريبا، بما في ذلك "سيجنال" و "بيب".
- التشفير والأمان وحذف الملفات والحفاظ عليها جيد عند واتس اب مقارنة بالمنصات الأخرى، وهناك دراسة تذكر أن الخصوصية والأمان في الواتس اب تتساوى مع تطبيق سيجنال، فيما يأتي في المرتبة الأخيرة "تيلجرام" الذي يُتداول على أنه الأقوى مع العلم بأن المحادثات العادية والمجموعات والقنوات في تيلجرام غير مشفرة بنظام "تشفير طرف لطرف" الأكثر أمنا.
- النسخة الاحتياطية لواتس واب لا تخزن في مكان واحد فقط، فهناك نسخة داخل الجهاز، وأخرى محملة على السحابة التخزينية في حساب قوقل، وخاصية المزامنة التلقائية تجعلها محفوظة كاملة على السحابة التخزينية، فيجب إلغاء المزامنة التلقائية أو على الأقل توقيف المزامنة التلقائية للواتس اب إذا لم ترغب بذلك.
- عند الحديث عن الخصوصية يجب تحقيق الأمان على أجهزة المستخدمين أولاً ومن ثم على التطبيقات والمنصات المثبتة على هذه الأجهزة، فالبيانات المخزنة على جهازك غير مشفرة.
- سلوك المستخدم هو الذي سيحدد الأمان في التعاطي مع هذه التطبيقات.
- يرى م. مشتهى أنه لا مشكلة في استخدام الواتس اب في إطار الاستخدام العادي البسيط والتواصل العائلي وما شابه ذلك، وسيستمر في تواجده عبر واتس اب، والأفضل من ذلك كله أن يكون هناك منصة أو تطبيق خاصة بنا.

الزاوية الأولى: أمان التطبيق/

- لا يوجد أمان لأي تطبيق موصول بشبكة الانترنت "بحيث لا نترك الأمور على الغارب"، ولكن "ما لا يدرك كله، لا يترك جله".
- مشكلة الواتس اب ليس في الرسائل المشفرة إنما البيانات الأخرى الشخصية، وإن كانت النسخ الاحتياطية ليست مشفرة فيه.
- تليجرام آمن لكن ليس كما يظن البعض، فالواتس اب يعتبر أكثر أماناً نسبيا، أما الأمان الجيد في تليجرام فهو في "المحاثات السرية فقط" فهي التي تكون "مشفرة من طرف لطرف"، أما المحادثات العادية والمجموعات فهي "غير مشفرة تشفير من طرف لطرف".
- سيغنال هو أفضل الموجود حاليا بالنسبة للبرامج المطروحة.

الزاوية الثانية: محافظة التطبيق على الخصوصية/

- الفيس بوك من أسوأ الشركات في خصوصية البيانات ولها فضائح كثيرة، الخطورة في أنها تجمع المعلومات وتبيعها سواء للإعلانات التجارية أو -وهذا هو الأخطر- صناعة وتوجيه الرأي العام كما حدث في الانتخابات الأمريكية.
- أنت مجبر على أن تشارك معلوماتك مع الفيس بوك خلال الفترة التي حددتها الواتس اب أو تحذف حسابك. لا يوجد خيار.

الزاوية الثالثة: إمكانية الاختراق/

- ✓ جانب الاختراق موضوع منفصل ومختلف عن موضوع الخصوصية وجمع البيانات بطريقة قانونية.
- ✓ الكل معرض للاختراق، لا نتحدث فقط عن اختراق الجهاز، بل عرضة البرنامج نفسه للاختراق. فكل البرامج تقريبا في هذا الأمر سواء، كلها معرضة للاختراق.
- ✓ كل البرامج تظهر فيها بشكل مستمر ثغرات يمكن أن تستغل أمنياً، لذلك بعض التطبيقات ترسل تحديثات أمنية بشكل دوري لردم كل هذه الثغرات. ومهم للمستخدمين مواكبة هذه التحديثات والتأكد من استخدامهم دائما النسخة الأخيرة من التطبيق.

- ✓ يوجد أنواع أخرى من الثغرات تكتشفها جهات معينة تستغلها وتصل الى تلك البيانات وقد تبقى هذه الثغرة غير معروفة إلا إذا تم الكشف عن هؤلاء الناس أو عَرف مُطوّروا التطبيق عن هذه الثغرة وردموها. فلا مهرب كامل من الاختراقات.
- ✓ الفيس بوك يقوم بعمل معالجة للبيانات، فإن تم أي اختراق لذلك يستطيع المخترق أن يصل لكل البيانات المعالجة والجاهزة بشكل سهل وبسيط.

وفيما يتعلق بمسألة البديل الأفضل تحدث م. صيام بأن ذلك متعلق باختيار كل شخص بما يناسبه بعد توضيح الأمان وسياسة الخصوصية والمخاطر في كل تطبيق، ويرى أن تطبيق السيجنال هو الأفضل بين التطبيقات المتاحة، ويرى أن مغادرة واتس اب سيشكل ضغطا على الشركة للتوقف عن تنفيذ سياسة الإجبار ضد المستخدمين.

أما بخصوص التطبيق التركي "بيب" فمن الناحية الفنية والتقنية تظهر الأمور التالية: المعلومات غير كافية عنه، المعلومات التي يجمعها نفس الواتس تقريبا، موضوع التشفير غير واضح لحد الآن، قانونيا لا يظهر لمن يتبع بشكل واضح.

مداخلة أ. خالد صافي المختص في التسويق الرقمي

المحتوى الفلسطيني محارب من الكثيرين على الانترنت، من القائمين على المنصات أو الذباب الإلكتروني، وهناك خوارزميات خاصة بالكلمات المفتاحية المرفوضة التي تسبب الحظر والحذف.

- المحاربة تتم للإعلاميين الفلسطينيين وصفحاتهم ومحتواهم حتى وإن تم توثيقها وأخذ العلامة الزرقاء، ويتم محاربتهم بالحذف النهائي للصفحات والحسابات الخاصة بهم.
- الشخص المحذوف من فيس بك يتم حذفه من انستغرام حتى لوم يربط حسابه.
- الفلسطيني يجب أن يحاول التواجد دائما مهما تم حذفه، وأن يتحدث عن حياته كرسالة بدون استخدام المصطلحات السياسية أو المحظورة، وهو الحل البديل المتاح حاليا.
- واتساب يقوم بحذف بعض الحسابات بناء على بعض المحادثات الخاصة بالمستخدمين.
- فيس بوك أسوأ من يستخدم البيانات.
- تم مواجهة ذلك في روسيا فصنعوا منصة بديلة للفيس وهي المعتمدة هناك بدلا للفيس، وأنشؤوا سيجنال بدل الواتس اب أيضا، ومثال آخر لتطبيق حديث ومنافس وهو تيك توك.

- لذلك نحن بحاجة إلى تطبيق فلسطيني أو عربي أو مسلم حتى ننشر الرواية الفلسطينية دون محاربة، حيث أننا ربما حين ننتقل لحسابات ومنصات أخرى من الوارد جدا أن تقوم بتغيير سياستها لاحقا بما يحارب المحتوى الفلسطيني.
- الاتحاد الأوربي مستثنى من هذا الشرط الحديث لواتس اب بسبب وجود قانون يمنع مثل هذه الشركات من هذه السياسات.
- هذه البيانات التي يتم جمعها عن الحسابات يمكن تقديمها للحكومات في حال طلبها، والآن واتس اب ستشارك بيانات المشتركين مع فيس بوك التي تقوم بتقديم المعلومات والبيانات للحكومات في حال رأت ذلك.
- كل تطبيق تشرف عليه حكومة يكون فيه مخاوف كبيرة، والأفضل ألا يكون تابعا للحكومات.
- البيانات قد تكون آمنة وعادية لكن يتم حفظها ومعالجتها واستخدامها في أغراض تسويقية.
- فيس بوك سيقوم باستخدام بيانات الواتس اب التي كانت لديه بعد ٨ فبراير بكل الأحوال.
- البديل المطروح هو سيجنال الذي هو أقل التطبيقات طلبا للبيانات، وتشفيره مثل واتساب، لكن من سلبياته بأنه لا يوجد فيه رموز تعبيرية.
- تيلجرام قال بأن لديه ٢٥ مليون مستخدم جديد، فهو الأوفر حظا في هذه المرحلة، لكن نذكر بأنه لابد من تشغيل تشفير الرسائل يدويا من الخلال التحدث عبر خاصية (الرسائل السرية).
- أنا أفضل تطبيق pip التركي، وقد جمع ٥ مليون مشترك جديد خلال الأيام القليلة السابقة.
- (فيسبوك مسنجر انستغرام واتس اب) كلها عائلة واحدة، فإذا كنت ستستخدم أحدا منها ستعطي نفس الأذونات التي ستعطي نفس البيانات.

مداخلة أ. إياد القرا حول اطلاق أدوات تقنية جديدة لمواجهة محاربة المحتوى الفلسطيني:

أوضح أ. إياد القرا –رئيس المركز الشبابي في غزة- أنهم بعد رصد وإعداد قوائم بالمصطلحات الفلسطينية الوطنية -الخوارزميات- التي يُستهدف مستخدميها من قبل إدارات منصات الإعلام الإجتماعي، قاموا بالعمل على إعداد أداة تستخدم عبر الهواتف المحمولة وأداة أخرى تستخدم عبر متصفح كروم، كخطوات تقنية وعملية لمواجهة الحرب المفتوحة على المحتوى الفلسطيني على مواقع الإعلام الإجتماعي خاصة الفيس بوك، وسيتم الإعلان علن عن إطلاقهن في الأيام القريبة، وحول آلية عملهن قال "بعد تفعيل ربطهما بمنصات التواصل سيعملان على إشعار كاتب المحتوى الفلسطيني حول الكلمات والمصطلحات المستهدفة؛ ثم سيرشحان -التطبيق والأداة- له بعض الطرق إما باستبدال المصطلح أو العمل على ترميزه وتقطيعه آلياً ".