EUPOL COPPS
البعثة الاوروبية لمساندة الشرطة الفلسطينية

الشرطة
POLICE
Palestinian Police
الشرطة الفلسطينية

الشرطة الفلسطينية
وحدة الجرائم الإلكترونية

نبذة

في الوقت الذي أصبحت فيه شبكة الإنترنت تنتشر بشكل واسع لتصل لجميع الأفراد والمؤسسات، ارتفع معدل الجرائم الإلكترونية وباتت تهدد أمن وسلامة كل مستخدميها، ومع تزايد استخدام شبكة الإنترنت في عمليات التجارة الإلكترونية سوف تتزايد صور تلك الاعتداءات والتهديدات مما دفعنا إلى الإقرار بوجود هذه الجريمة والتنبيه بخطورتها وضرورة أخذ موقف صارم لمحاربتها، وإيجاد حلول مناسبة لها، ومن هنا صدرت تعليمات السيد اللواء/ حازم عطا الله مدير عام الشرطة في مطلع العام 2013، بإنشاء وحدة مختصة لمواجهة هذه الجريمة تسمى **وحدة الجرائم الإلكترونية** تتبع لإدارة المباحث العامة.

مهام وحـدة الجرائـم الإلكترونيـة

- متابعة كافة قضايا الجرائم الإلكترونية والتحقيق فيها
- فحص وتوثيق وتحليل الأدلة الرقمية المرتبطة بالجرائم الإلكترونية والجرائم التقليدية
- نشر التوعية والثقافة اللازمة لكافة فئات المجتمع في مجال الجرائم الإلكترونية
- المساعدة الفنية لإدارة المباحث العامة وأفرع المباحث في المحافظات وإدارات ومديريات الشرطة المختلفة

بلغ عدد الشكاوي
التي تم التعامل معها
خلال عام 2018
من قبل
وحدة الجرائم الإلكترونية

2568
شكوى

بزيادة وصلت (26.6%)
عن عام 2017

الابتزاز الإلكتروني

عملية تهديد وترهيب بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلالها للقيام بأعمال غير مشروعة.

كيف يحصل الابتزاز

- إرسال طلبات صداقة للضحايا من حسابات وهمية عبر مواقع التواصل الاجتماعي
- إنشاء علاقة ثقة ومن ثم تنتقل للتواصل عبر تطبيقات المحادثات المرئية
- استدراج الضحية للحصول على صور خاصة وتسجيل أي محتوى مسيء
- يقوم المشتبه به بعملة التهديد والابتزاز مقابل دفع مبلغ مالي أو القيام بأعمال غير مشروعة

كيف تقي نفسك

- احرص على إضافة الأشخاص الموثوقين، ولا تجعل حسابات التواصل الاجتماعي الخاصة بك مرتع لمن لا تعرفهم
- تجنب نشر معلوماتك الشخصية وأنشطتك اليومية، فهنالك من يتربص لاستغلالها بطريقة قد تجلب لك المتاعب
- اقرأ وافهم إعدادات الخصوصية في شبكة التواصل الاجتماعي التي تستخدمها، وقم بتعطيل خدمة "المكان" التي تكشف مكانك عند وضعك أية تغريدة أو ملاحظة
- احرص على قراءة الرابط والتأكد من أنه يأخذك إلى الموقع الأصلي وليس موقع مزيف
- احرص على استخدام البرامج المعتمدة من الشركات الرئيسية
- تجنب الضغط على الروابط قدر الإمكان، ولا تضغط على أي روابط من أشخاص لا تعرفهم

في حال كنت ضحية لأحد الجرائم الإلكترونية

1. توقف عن الحديث مع المجرم تماماً
2. السيطرة على الانفعالات والتصرفات لاتخاذ القرار السليم
3. وثق كافة المراسلات والجرم المرتكب ورابط حساب المجرم
4. لا تتردد بالتوجه إلى أقرب مركز شرطة لتقديم شكوى رسمية لكي تتم مساعدتك والوصول إلى المجرم

تأمين حسابك عبر مواقع التواصل الاجتماعي

- ربط الحساب برقم هاتف فعال، وتفعيل التحقق بخطوتين لزيادة مستوى الحماية
- التأكد من ربط الحساب ببريد إلكتروني فعّال
- اختيار كلمة مرور قوية، بشكل دوري وتغييرها بشكل دوري
- إضافة أصدقاء موثوقين وإخفاء قائمة الأصدقاء
- قم بتثبيت أحدث الإصدارات من المتاجر الرسمية فقط
- تجنب التواصل مع أشخاص غير موثوقين
- لا تخبر أحداً عن بريدك الإلكتروني الخاص بالمنتديات ومواقع التواصل الاجتماعي
- لا تستخدم بريدك الإلكتروني الخاص بالعمل للأغراض الشخصية
- لا تضغط على أي رابط يصلك عبر البريد الإلكتروني، ولا تقم بتحميل الملفات المرفقة إلا من الأشخاص الموثوقين

أمن الهواتف

- احـرص علـى تحديـث نظـام تشـغيل جهـازك الذكـي باسـتمرار
- احرص على تحميل التطبيقات والبرامج من المتاجر المعتمدة فقط
- قـم بتعطيـل خاصيـة الاتصـال التلقائـي علـى الشـبكات اللاسـلكية وإغـلاق البلوتـوث
- احـرص علـى حمايـة جهـازك الذكـي بكلمـة مـرور أو نقـش أو عـن طريـق البصمـة
- تأكـد مـن تفعيـل خاصيـة "القفـل التلقائـي" للجهـاز
- احـرص علـى تفعيـل خاصيـة "إيجـاد مكانـي" وذلـك للعثـور علـى الجهـاز فـي حـال تـم فقدانـه
- احـذر مـن شـراء الأجهـزة مـن الأماكـن الغيـر موثوقـة
- لا تقم بكسر حماية جاهزك "Rooting, JailBreak" مهما كانت الأسباب
- لا تضـع معلومـات حساسـة علـى هاتفـك قـد تعرضـك للخطـر

أمن الحاسوب

- قم بتغير الإعدادات الافتراضية وتعطيل أية خدمات لا تستخدمها في نظام التشغيل
- قم بتنصيب برامج معتمدة مضادة للبرمجيات الخبيثة (Anti Virus) وقم بتفعيل (الجدار الناري) لتجنب أي اختراق
- قم بتحديث برامجك ونظام التشغيل وبرامج الحماية باستمرار للحصول على الحماية ضد أية مخاطر
- قم بأخذ نسخ احتياطية لمعلوماتك بشكل دوري ولا تحفظها في مكان واحد فقط
- قم بقفل الجهاز (lock) في أوقات الاستراحة لتجنب دخول أي شخص غير مخول وقم بتسجيل الخروج (Log Off) عند الانتهاء من العمل

أفضل الطرق
لأمن الشبكات اللاسلكية

- أنت المسؤول الأول عن شبكتك اللاسلكية، فاحرص على حمايتها بكلمة مرور قوية ذات تشفير عالي، وتأكد دائماً من يستخدمها
- قم بتغيير كلمة المرور الافتراضية الخاصة بصفحة الراوتر، وقم بتغيير اسم الشبكة الافتراضي
- لا تعط كلمة المرور الخاصة بشبكتك إلا للأشخاص الموثوقين
- لا تثق بالشبكات المجانية وكن حذراً عند الاتصال بها

Free Tel: 100

www.palpolice.ps

PalestinianPolice1