سياسة الحماية من التدخل الإلكتروني والمراقبة

أولاً: كيفية التصرف أثناء الاستدعاء الأمني للتحقيق.

1) ابلاغ أحد الزملاء من مجلس الادارة أو الاعضاء.
2) التواصل مع العائلة لمعرفة آخر الأخبار.
3) التواصل مع احد المحامين، بالتنسيق مع الأهل، يفضل أن يقوم العضو بعمل توكيل رسمي لأحد المحامين الموثوقين بشكل دائم وأبلاغ الجمعية بأسم المحامي.
4) في حالة عدم اتصاله بأهله وتحديد مكان تواجده، ابلاغ المؤسسة الوطنية لحقوق الانسان.
5) تتولى نقطة الاتصال الأمني التواصل مع الشفافية الدولية، فرونت لاين ديفندرز، الجمعية البحرينية لحقوق الانسان، مفوضية حقوق الأنسان في بيروت.

ثانياً: حماية البريد الإلكتروني:

1) استخدام كلمات مرور قوية ومعقدة، تحتوي على مزيج من الأحرف والأرقام والرموز، ويتم تغييرها بشكل دوري.
2) تفعيل المصادقة الثنائية، لزيادة مستوى الأمان.
3) تجنب فتح الروابط المريبة والملفات المرفقة من مصادر غير معروفة.
4) تفعيل أنظمة الحماية المتوفرة في البريد الأليكتروني.

ثالثاً: حماية الهاتف.

1) اعتمد خاصية اغلاق الهاتف بشكل تلقائي كل 30 ثانية مثلاً.
2) استخدام كلمات مرور أو البصمة لإعادة فتح الهاتف.
3) تفعيل التشفير، لحماية البيانات المخزنة.
4) تجنب تنزيل تطبيقات غير موثوقة، من مصادر غير معروفة.
5) تحديث نظام التشغيل والتطبيقات، بانتظام.

رابعاً: المراقبة والتجسس.

1) استخدام برامج مكافحة الفيروسات، لاكتشاف وإزالة البرامج الضارة.
2) تجنب الاتصال بشبكات Wi-Fi العامة غير الآمنة.
3) مراجعة أذونات التطبيقات، للتأكد من عدم الوصول غير المصرح به.

خامساً: التعامل مع الحوادث.

1) الإبلاغ عن أي نشاط مشبوه إلى الجهات المعنية.
2) تغيير كلمات المرور فورًا إذا تم الاشتباه في اختراق.
3) إجراء نسخ احتياطي للبيانات، بانتظام.

سادساً: أفضل الممارسات لحماية البيانات الشخصية.

1) كتابة كلمات مرور صعبة تحتوي على مزيج من الأحرف والأرقام والرموز.
2) تجنُّب استخدام المعلومات التي يسهل تخمينها، مثل أعياد الميلاد أو أسماء الأقارب القريبين.
3) استخدام كلمة مرور مختلفة لكل حساب.
4) ضرورة إجراء نسخ احتياطي دوري لبياناتك على محرك أقراص خارجي ستحتفظ به في مكان آمن أو ضمن بيئة تخزين سحابي آمنة.
5) انتبه لما تشاركه على منصات التواصل الاجتماعي والمواقع العامة الأخرى.
6) تجنب المشاركة غير الضرورية للمعلومات الحساسة أو الشخصية مع أطراف أخرى.
7) تجنب منح حق الوصول غير الضروري إلى بياناتك الشخصية لجهات غير معلومة لك.
8) أهمية المراجعة الدورية لبيانات البنك وبطاقة الائتمان الخاصة بك بحثاً عن أي نشاط غير مصرح به.
9) قم بمراجعة كشوف حساباتك سواء البنكية أو بطاقة الأئتمان.
10) التخلص من البيانات بشكل آمن.
11) احرص على تمزيق المستندات المادية التي تحتوي على معلومات شخصية قبل التخلص منها.

سابعاً: تمكين المصادقة الثنائية(FA2)

1) تفعيل المصادقة الثنائية متى ما أمكن ذلك، لإضافة طبقة أمان إضافية.
2) يتضمن هذا عادةً تلقي رمز (مثل كلمة المرور لمرة واحدة) على هاتفك أو بريدك الإلكتروني للتحقق من هويتك، في كل مرة تحاول فيها تسجيل الدخول إلى حسابك.
3) تحديث البرامج بشكل دوريّ.
4) تحديث نظام التشغيل والتطبيقات وبرامج مكافحة الفيروسات بانتظام لمعالجة نقاط الضعف.

ثامناً: الحذر من التصيُّد الاحتيالي.

1) الحذر من رسائل البريد الإلكتروني أو الرسائل أو المكالمات غير المرغوب فيها، والتي تطلب معلومات شخصية.
2) عدم النقر على الروابط المشبوهة أو تنزيل المرفقات من مصادر غير معروفة.

تاسعاً: شبكات واي فاي الآمنة

1) استخدام كلمات مرور قوية لشبكات واي فاي الخاصة بك.
2) إلغاء تفعيل إعداد واي فاي المحميWPS ، نظراً لقابليته للاختراق.

عاشراً: التأكد من الاتصال التكنلوجي الآمن

1) عند تقديم معلومات شخصية عبر الإنترنت، تأكد من أن الموقع الإلكتروني يستخدم بروتوكول نقل النص التشعبي الآمن HTTPS ابحث عن رمز القفل إلى جوار الرابط.
2) تحقق من الأذونات التي تطلبها التطبيقات قبل تثبيتها.
3) تجنب منح حق الوصول غير الضروري إلى بياناتك الشخصية.
4) استخدم خدمات معروفة وذات موثوقية عالية من أجل المعاملات عبر الإنترنت وتخزين البيانات.

على الرغم من هذه النصائح في تعزيز أمان بياناتك بشكل كبير، إلا أنه لا توجد طريقة مضمونة بالكامل. كن متنبّهاً واستمر في التعرف على إجراءات أمن المعلومات الجديدة التي تواكب التطور التكنولوجي.