نصائح سريعة:

- حماية البيانات الهامة بتفعيل النسخ الاحتياطي التلقائي وبشكل متعدد مشفر ومنتظم.
- تثبيت برامج مكافحة الفيروسات وتحديثها باستمرار.
- زيادة الوعي المؤسسي بالأمن السيبراني.
- عند القيام بأنشطة مالية عبر الإنترنت مثل التحويلات المصرفية، تأكد من استخدام مواقع ويب مشفرة وآمنة.
- احذر من برامج الفدية والخداع الاحتيالي.
- قم بإنشاء كلمات مرور فريدة وقوية واستخدام المصادقة متعددة العوامل الثنائية.
- قم بالنظر في خيارات التأمين السيبراني.
- كن حذرًا عند اختيار موفري خدمات تكنولوجيا المعلومات.
- تأمين اتصالات البريد الإلكتروني الخاصة بك عن طريق تشفير رسائل البريد الإلكتروني الحساسة.
- مراقبة أنشطة المتطوعين المشبوهة.
- تأكد من أن مؤسستك لديها حلول أمنية مثل جدران الحماية وبوابات البريد الإلكتروني وأنظمة منع وكشف التسلل IDS / IPS قبل وعند حدوث الهجمات الإلكترونية.
- قم بإدارة المخاطر البشرية من خلال الاستثمار في التوعية والتثقيف حول مخاطر الأمن السيبراني.