تثقيف المستخدمين: نشر الوعي حول مخاطر الأمن السيبراني: ـ شرح أنواع التهديدات الإلكترونية الشائعة، مثل التصيد .1 الاحتيالي والبرامج الضارة وبرامج الفدية. ـ توعية المستخدمين بتأثير هذه التهديدات على الأفراد والمنظمات. تقديم إرشادات حول حماية النفس والأجهزة: ـ تعليم المستخدمين كيفية إنشاء كلمات مرور قوية وفريدة من نوعها. ـ التأكيد على أهمية تحديث البرامج وتثبيت برامج مكافحة الفيروسات. تعزيز ثقافة الإبلاغ عن الحوادث: ـ تشجيع المستخدمين على إبلاغ قسم تكنولوجيا المعلومات أو فريق الأمن عن أي نشاط مشبوه. ـ التأكيد على سرية التقارير وحماية هوية المبلغين. 2. تعزيز الممارسات الجيدة: دمج ممارسات الأمن السيبراني في الثقافة اليومية: ـ تشجيع استخدام كلمات مرور قوية وفريدة من نوعها على جميع الحسابات. ـ تذكير المستخدمين بضرورة تحديث البرامج وتثبيت برامج مكافحة الفيروسات بانتظام. توفير أدوات ودورات تدريبية: ـ تسهيل الوصول إلى أدوات إنشاء كلمات المرور وتشفير البيانات. ـ تقديم دورات تدريبية منتظمة حول الأمن السيبراني للموظفين والمتدربين. ـ نشر مواد توعوية عبر قنوات التواصل الداخلية للمنظمة. 3. كشف التهديدات: ـ شرح علامات البريد الإلكتروني والرسائل النصية المشبوهة. ـ توعية المستخدمين بمخاطر مواقع الويب المزيفة والتصيد الاحتيالي. ـ تعليم المستخدمين كيفية التحقق من صحة الروابط قبل النقر عليها. تزويد المستخدمين بأدوات للكشف عن التهديدات: ـ توفير برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة. ـ تثبيت أدوات حظر الإعلانات وتتبع المواقع الإلكترونية. أهمية التحقق الثنائي: 1. طبقة إضافية من الأمان: يُضيف طبقة حماية إضافية إلى حسابات المستخدمين: مثل كلمة المرور ورمز يتم إرساله إلى هاتف المستخدم أو جهاز آخر. يجعل من الصعب على المتسللين الوصول إلى الحسابات حتى لو تمكنوا من الحصول على كلمة المرور. يُقلّل من مخاطر سرقة الحسابات: