



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

حماية حسابي وملفاتي على المنصة التعليمية

الحذر من الرسائل الاحتيالية والروابط المشبوهة:

كن حذرًا عند فتح رسائل البريد الإلكتروني أو الرسائل النصية المشبوهة التي تطلب منك تسجيل الدخول على المنصات التعليمية أو تقديم معلومات خاصة. فيجب عليك التحقق الدائم من مصدر الرسالة قبل اتخاذ أي إجراء.



التحقق من سياسات الخصوصية:

تحقق من سياسات الخصوصية والأمان المتعلقة بالمنصات التعليمية التي تستخدمها. تأكد من أن المنصة تتبع ممارسات أمان قوية وتحمي معلوماتك الخاصة بشكل صحيح.



النسخ احتياطي بشكل دوري:

قم بإنشاء نسخ احتياطية لملفاتك الهامة على المنصات التعليمية باستخدام خدمات التخزين السحابي أو وسائط تخزين خارجية لتجنب فقدانها.



كن على اطلاع

تأكد من قراءة واتباع أي تعليمات أو إرشادات أو تنبيهات أمنية تقدمها المنصة التعليمية لضمان استخدامها بشكل آمن.



عزيزي الطالب،

باتباعك لهذه الإرشادات السيبرانية ستتمكن من حماية ملفاتك وحساباتك على المنصات التعليمية بفعالية أكبر وتقليل فرص تعرضك للمخاطر على الانترنت.

استخدم كلمات مرور قوية:

استخدم كلمات مرور قوية وفريدة لحساباتك على المنصات التعليمية تحتوي على مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز. وتجنب استخدام كلمات سهلة التخمين أو تحتوي على معلوماتك الشخصية.



تفعيل المصادقة الثنائية:

قم بتفعيل خاصية المصادقة الثنائية (2FA) على حساباتك عندما تكون متاحة، فهذه الخاصية تضيف طبقة أمان إضافية وذلك من خلال طلب رمز تأكيد إضافي عند تسجيل الدخول.



حماية البريد الإلكتروني:

تأكد من تأمين حساب بريدك الإلكتروني بواسطة كلمة مرور قوية وتفعيل المصادقة الثنائية إن أمكن، فالبريد الإلكتروني يعتبر بوابة للوصول إلى حساباتك الأخرى، لذا يجب حمايته بشكل جيد.



تحديث البرامج والتطبيقات:

تأكد من تحديث البرامج والتطبيقات الخاصة بالمنصات التعليمية بانتظام، ولا تنسى تحديث نظام التشغيل والبرامج والتطبيقات الأخرى لسد الثغرات الأمنية وحماية أجهزتك من الاختراق.



www.ncsc.gov.bh



ncsc_bh



ncscbh

مع تحيات المركز الوطني للأمن السيبراني