سايبر
MEWA

دليل إرشادات الأمن السيبراني
للمـــوظـــــف
Employee Cyber Security Guide

الإدارة العامة للأمن السيبراني
مـــركز التـــوعية والإرشـــاد

mewa_ksa 4555

وزارة البيئة والمياه والزراعة
Ministry of Environment Water & Agriculture

يسعدنا أن نقدم لكم بعض الإرشادات الأمنية.
شاكرين لكم حرصكم و اهتمامكم و نتمنى لكم دوماً التوفيق و النجاح.

We are pleased to you present you some security tips.
We thank you for your carene's and attention.and we Always wish you success.

عدم إستخدام أجهزة الحاسب الآلي أو أي اجهزة تقنية تابعة للوزارة لتنزيل و تنصيب البرامج التي ليس لها علاقة في بيئة العمل.

Not to use computers or technical devices affiliated with the Ministry, to download and install programs that have nothing to do with the work environment.

التأكد من عدم وجود أشخاص غير مخولين للحصول على المعلومات المعروضة في محيط شاشة الحاسب الآلي، مع أهمية تفعيل خاصية شاشة التوقف.

Ensure that there are no unauthorized persons able to obtain the information displayed in thevicinity of the computer screen with theimportance of activating the screen saver feature.

عدم نقل الملفات والمستندات التي تخص الوزارة خارج نطاقها خاصة السرية منها مهما اختلفت الوسائل و الطرق و الآليات.

Not to transfer files and documents belonging to the organization outside its scope , especially confidential ones, regardless of its means, methods and mechanisms.

عدم استخدام أجهزة خارجية أو شخصية داخل الوزارة إلا بتصريح من الإدارة العامة للأمن السيبراني.

Not to use external or personal devices inside the ministry without a permit from the General Department of Cyber Security.

يسعدنا أن نقدم لكم بعض الإرشـادات الأمنيـة.
شاكرين لكم حرصكم و اهتمامكم و نتمنى لكم
دوماً التوفيق و النجاح.

We are pleased to present to you some security tips.
We thank you for your carene's and
attention.And we Always wish you success.

التـــأكد من أن رسائـــل البـريد الإلـكتروني صـــادرة
من أشخـاص و جهات معروفة أو موثوقة ، مع ضرورة
فحص الملفـات والمـرفقات المرفقـــة قبـل فتـحها.

check that e-mails are from well-known or
trusted personnel's with the need to check
the attached files before opening them.

ضرورة الحفاظ على معلومات الدخـول و
عدم إفشاءها أو الإفصاح عنها لأي شخص.

The need to preserve the login
information and not disclose it
to anyone.

في حال الشك في أي سلوك تقني غير عـادي
يمكنـكم التواصل مع الرقم الخـاص بالدعـم و
البلاغات بالإدارة العامة للأمن السيبراني 4555.

In case of the suspicion of any unusual
technical behavior you can contact the
number for support and reports at the
General Department of Cyber Security
4555.

استخدام البريـد الإلكـتروني الخـاص
بالعمل في نطاق المهام المناطة فقط.

Use of work e-mail within the scope
of the tasks assigned to it.

يسعدنا أن نقدم لكم بعض الإرشادات الأمنية.
شاكرين لكم حرصكم و اهتمامكم و نتمنى لكم
دوماً التوفيق و النجاح.

We are pleased to present you some security tips.
We thank you for your eagerness and
attention.We Always wish you success.

أمن متصفح الانترنت

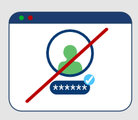
Internet Browser Security

حـــدِّث متصـفـح
الإنترنت باستمرار

Always keep your
browser update.

امنع و اغلق النوافذ المنبثقة
فبعضها قد تشكل تهديدات

Block and close pop-ups
Some of them may pose
threats.



احرص على عدم حفظ كلمات
المرور على المتصفح باختيار
تذكرني لأنه يمكن للمخترق
الحصول عليها عند اختراق الهاتف

Be sure not to memorize words
Choosing to navigate the browser
Remember me because the hacker
can Get it when hacking the phone

ثبـت متصفحـات الإنتـرنـت
من المواقع و المتاجر الرسمية

Install internet browsers
From official websites and
stores.

استخدم متصفحات
الإنترنت المعروفة

Use browsers
Known Internet

حماية حساباتك عبى مواقع التواصل

Protect your accounts on social media

حمل البرامج من
المتجر الرسمي

Download software
from official store.

استخدم كلمة
مرور قـويـة

use strong
password.

تفعيـل خاصـية التحـقـق
الثنائي عند الدخول للحساب

Activate two-factor
authentication.

عـدم مـشـاركـة
المعلومات الشخصية

Do Not disclose
personal information.

التأكد من سلامة الروابط
و الملفات قبل فتحها

Ensure URLs and files
are safe.

We are pleased to present you some security tips.
We thank you for your eagerness and attention.We Always wish you success.

يسعدنا أن نقدم لكم بعض الإرشادات الأمنية.
شاكرين لكم حرصكم و اهتمامكم و نتمنى لكم دوماً التوفيق و النجاح.

Beware of Phishing Email

أحذر التصيد الالكتروني

Phishing Email is an attempt to obtain sensitive information such as user names, passwords or credit card details, often for malicious reasons by disguising as a trustworthy organization in Email messages.
Some Effective Ways to Detect Phishing:

التصيد الإلكتروني هو محاولة الحصول على معلومات حساسة مثل بعض أسماء المستخدمين و كلمات المرور أو تفاصيل بطاقة الائتمان غالبًا لأسباب و نوايا ضارة و خبيثة و ذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية
بعض الطرق الفعالة لرصد التصيّد:

Disguised or modified links

Moving the mouse over the link without clicking
It Shows the actual URL you are directed to e.g .
such as: www.mewa.gov.sa

روابط مخفية أو معدلة

تمرير مؤشر الماوس على الرابط بدون الضغط عليه
سيكشف لك عنوان URL الفعلي الذي يتم توجيهك إليه
مثال:

Bad Grammar & Spelling

Poorly written sentences, bad grammar, and misspelled words indicate a phishing scam.

أخطاء إملائية

وجود أخطاء إملائية و نحوية واضحة غالباً ما يدل على عملية احتيال

Personal Information

Be ware of any messages that ask for your personal information.

المعلومات الشخصية

انتبه من أي رسائل تطلب منك توفير معلوماتك الشخصية

Logos or Signature

Don’t assume an email is legitimate because it includes official looking graphics.

الشعارات أو التوقيع

وجود صور لشعارات رسمية لا يدل على مصداقية المرسل

يسعدنا أن نقدم لكم بعض الإرشـادات الأمنيـة.
شاكرين لكم حرصكم و اهتمامكم و نتمنى لكم
دوماً التوفيق و النجاح.

We are pleased to present you with some security tips.
We thank you for your eagerness and
Attention. We Always wish you success.

أمن الأجهزة المحمولة

Mobile Devices Security

يجب الانتباه إلى الأجهزة المحمولة بشكل خاص حيث أن التطور المتـزايد فـي استخـدام الهـواتـف المحمولة جعل المتسلـلـون يسعون للسيطـرة على هذه الأجهزة بهدف للوصول إلى بيانـات المستخدمين و المؤسسات و العبث بها
للحماية من تهديدات الأجهزة المحمولة:

Mobile devices are something we should pay attention to, and With the growing sophistication of cell phones, hackers are trying to get their hands on any of these devices to access and manipulate users and organizations' data

تفعيل القفل الآلي
للأجهزة المحمـولة

Enable Mobile
Devices locking

تجنب الشبكات
المفتوحة

Avoid open networks

استخدم ميزة تتبع
الأجهزة المحمولة

Use mobile
tracking feature.

قم بتثبيت التطبيقات
من مـصـادر موثوقـة

Install applications
form trusted sources.

اسـتـخـدم بـرامـج
مكافحة الفيروسات

Utilize antivirus
software.

النسخ الاحتياطي
للبيانات بانتظـام

Backup data
regularly.

يسعدنا

دعمكم و إرشادكم في الأمن السيبراني

Secawareness@mewa.gov.sa

4555

وزارة البيئة والمياه والزراعة
Ministry of Environment Water & Agriculture

mewa_ksa 4555

الإدارة العامة للأمن السيبراني
مـــركز التـــوعية والإرشـــاد