سايبر
MEWA

دليـل Guide

إرشـــادات أمنـــية
للمـــوظـــف الجديد

مركز التوعية و الإرشاد
الإدارة العامة للأمن السيبراني

mewa_ksa 4555

وزارة البيئة والمياه والزراعة
Ministry of Environment Water & Agriculture

أخي الموظف / أختي الموظفة

ترحب بكم أسرة الإدارة العامة للأمن السيبراني في وزارة البيئة و المياه و الزراعة و تهنئكم بانضمامكم إلى فريق العمل بالوزارة و نأمل أن يثمر انضمامكم معنا لنجاحات رائعة نتوج بها

و بهذه المناسبة يسرنا إطلاعكم على دور الإدارة العامة للأمن السيبراني، فالإدارة تعنى بتحديد السياسات و الإجراءات الأمنية الخاصة بالوزارة بالإضافة إلى تقديم مجموعة من الخدمات التي تهم، الموظف كمنصة عابر، نظام ملفاتي، وغيرها من الخدمات التي يمكنكم الإستفاده منها في نظام جاهز على الرابط التالي:

https://smartit.mewa.gov.sa/dwp/app/#/session/login?returnUrl=%2F

و نأكد بضرورة إبلاغ الإدارة العامة للأمن السيبراني في حال التحقق من اشتباه أو التحقق من حصول إختراق أو تجاوز للسياسات الأمنية للوزارة و ذلك على البريد الإلكتروني secinfo@mewa.gov.sa

ممتنين لكم دائما التوفيق و النجاح

.

Dear employees

The family of the General Department of Cybersecurity in the Ministry of Environment, Water and Agriculture welcomes and congratulates you on joining the Ministry's team. We hope that by joining us we will result in great successes that will crown the Ministry,

On this occasion, we are pleased to inform you about the course of the General Department of Cyber Security,as the department will be defining the security policies and procedures of the ministry, in addition to providing a set of services of interest, as AlAbeer platform, my file system, and other services that you can benefit from in aljahez system on the following link:
https://smartit.mewa.gov.sa/dwp/app/#/session/login?returnUrl=%2F
We stress the need to inform the General Department of Cyber Security in the event of suspicion on a breach or violation of the security policies of the Ministry, via e-mail:
secinfo@mewa.gov.sa

Wish you all the best of luck.

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.

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 personnels to obtain the information displayed in the computer screen, With the importance 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 Departmentof 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 you some security tips.
We thank you for your eagerness and
attention.We Always wish you success.

التـأكد من أن رسائـل البريد الإلكتروني صادرة
من أشخـاص و جهات معروفة أو موثوقة ، مع
ضرورة فحص الملفـات المرفقـة قبـل فتحـها.

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
informationand 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 .

استـخدام البريـد الإلكـتروني الخـاص
بالعمل في نطاق المهام المناطة فقط.

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

يسعدنـا

دعمكم و إرشـادكم في الأمـن السيبـرانـي

Secawareness@mewa.gov.sa

4555

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

التصيد الإلكتروني

Phishing Email is an attempt to obtain sensitive information such as some user names, passwords or credit card details, often for malicious reasons by disguising as a trustworthy organiztion 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 some security tips.
We thank you for your eagerness and
attention.We Always wish you success.

Mobile Devices Security

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

Particular attention should be paid to mobile devices
as the development The increasing use of mobile
phones is making intruders They seek to control
these devices in order to gain access to data Users
and institutions and tampering with them.
To protect against mobile threats:

النسخ الاحتياطي
للبيانات بانتظـام

Backup data
regularly.

اسـتـخـدم بـرامـج
مكافحة الفيروسات

Utilize antivirus
software.

قم بتثبيت التطبيقات
من مـصـادر موثوقـة

Install applications
form trusted sources.

استخدم ميزة تتبع
الأجهزة المحمولة

Use mobile
tracking feature.

اتصـل بالإنـتـرنـت من
خلال شبكات موثوقة

Connect on the
internet through
trusted.

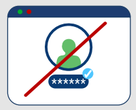
تفعيل القفل الآلي
للأجهزة المحمـولة

Enable Mobile
Devices locking

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 some security tips.
We thank you for your eagerness and
attention.We Always wish you success.

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 كلـمـات
المرور على المتصفح باختـيـار
تذكرني لأنه يمكن للمختـرق
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

Protect your accounts on social media

حمل البرامج من
المتجر الرسمـي
Download software
from official store.

استخدم كلمة
مرور قـويـة
use strong
password.

تفعيـل خاصـية التحـقـق
الثنائي عند الدخول للحساب
Use tow -factor-
authentication.

عـدم مـشـاركـــة
المعلومات الشخصية
Do Not disclose
personal information.

التأكد من سلامة الروابط
و الملفـات قبل فتـحـها
Ensure URLs and files
are safe.

مركز التوعية و الإرشاد
الإدارة العامة للأمن السيبراني

mewa_ksa 4555

وزارة البيئة والمياه والزراعة
Ministry of Environment Water & Agriculture