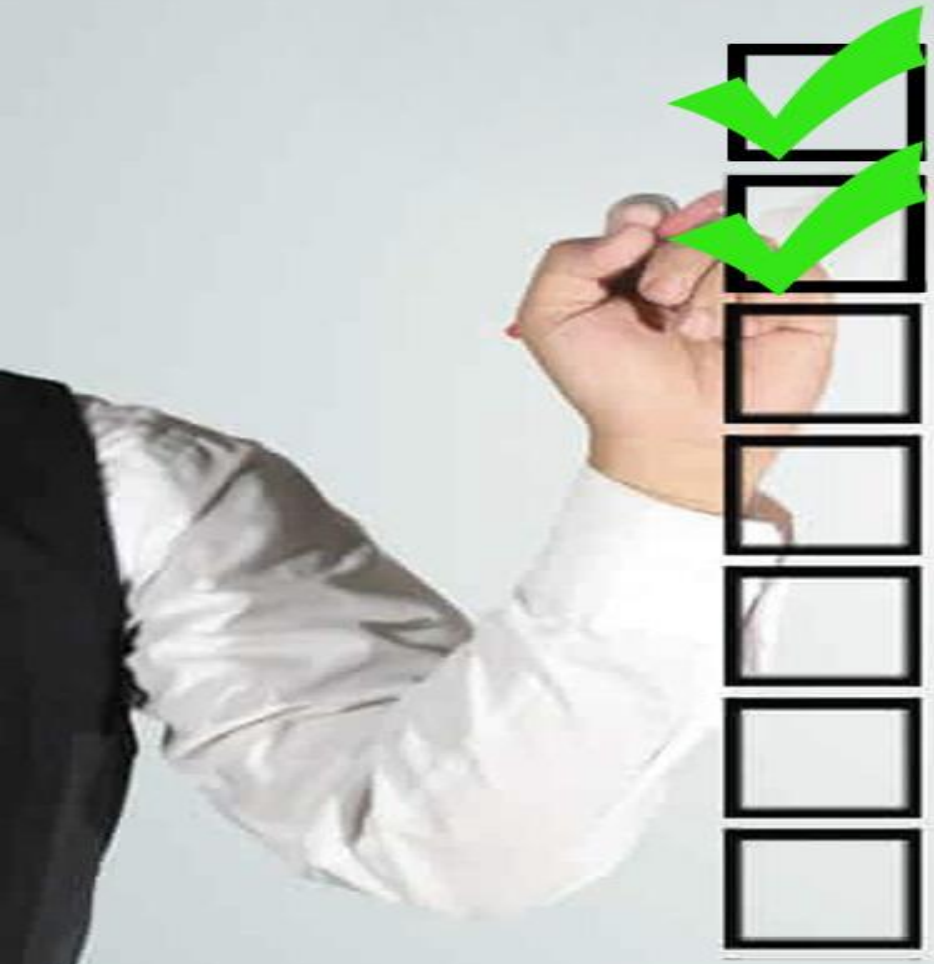
DELTA PHARMA

PHARAONIA
PHARMACEUTICALS

ابق بأمان أثناء عملك من المنزل

STAY SAFE .. WHILE WORKING AT HOME

أحمى جهازك .. اثناء عملك من المنزل

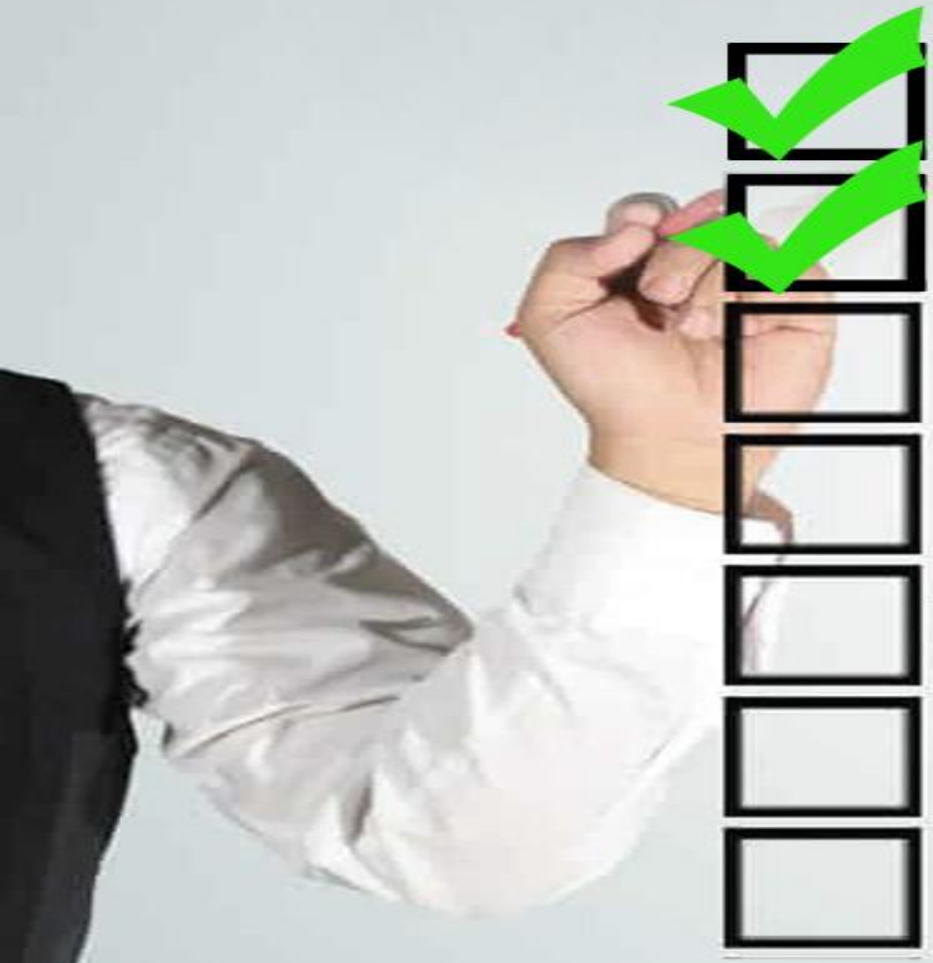


- [x] Use strong passwords
- [x] **Set up two-factor authentication**
- [ ] Use secure communication
- [ ] Set up firewalls
- [ ] Use an antivirus software
- [ ] Secure your home router
- [ ] Install updates regularly

EG | CERT

STAY SAFE .. WHILE WORKING AT HOME

أحمى جهازك .. اثناء عملك من المنزل

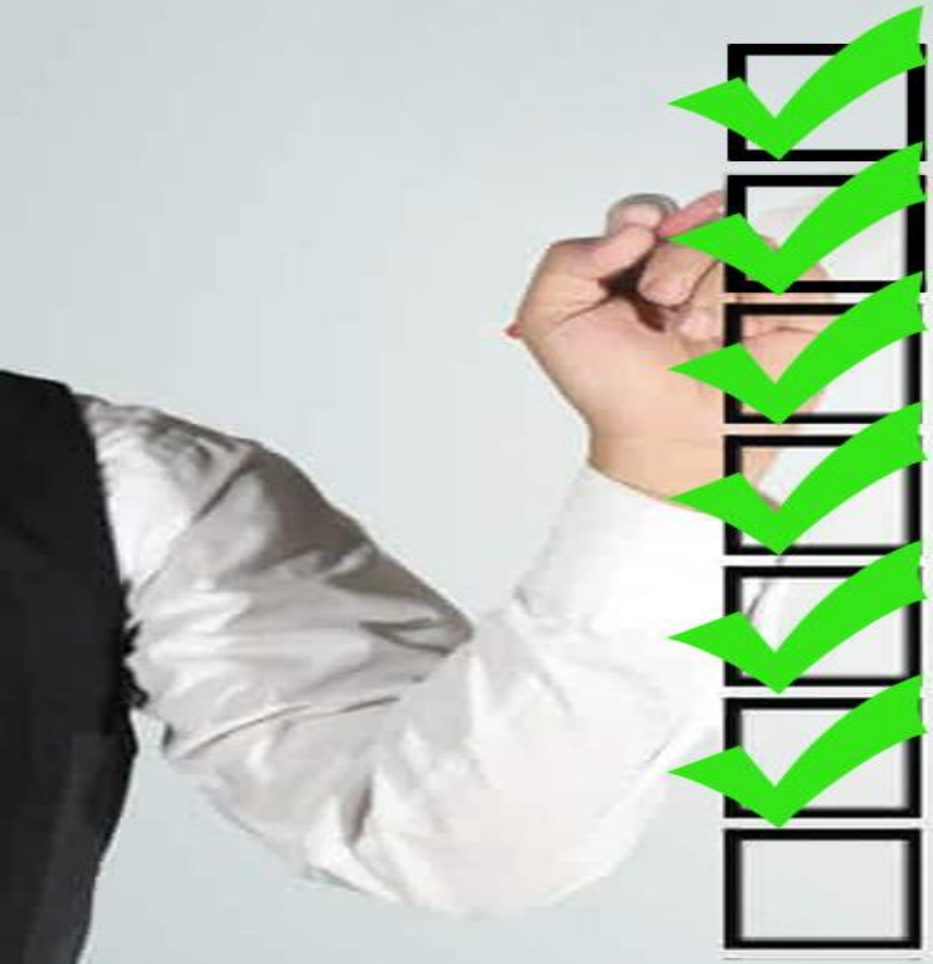


- [x] Install updates regularly
- [x] **Back up your data**
- [ ] Use log off
- [ ] Look out for phishing emails and sites
- [ ] Watch out for work-from-home scams
- [ ] Lock your device
- [ ] Restrict access to work devices

EG | CERT

STAY SAFE .. WHILE WORKING AT HOME

أحمى جهازك .. اثناء عملك من المنزل

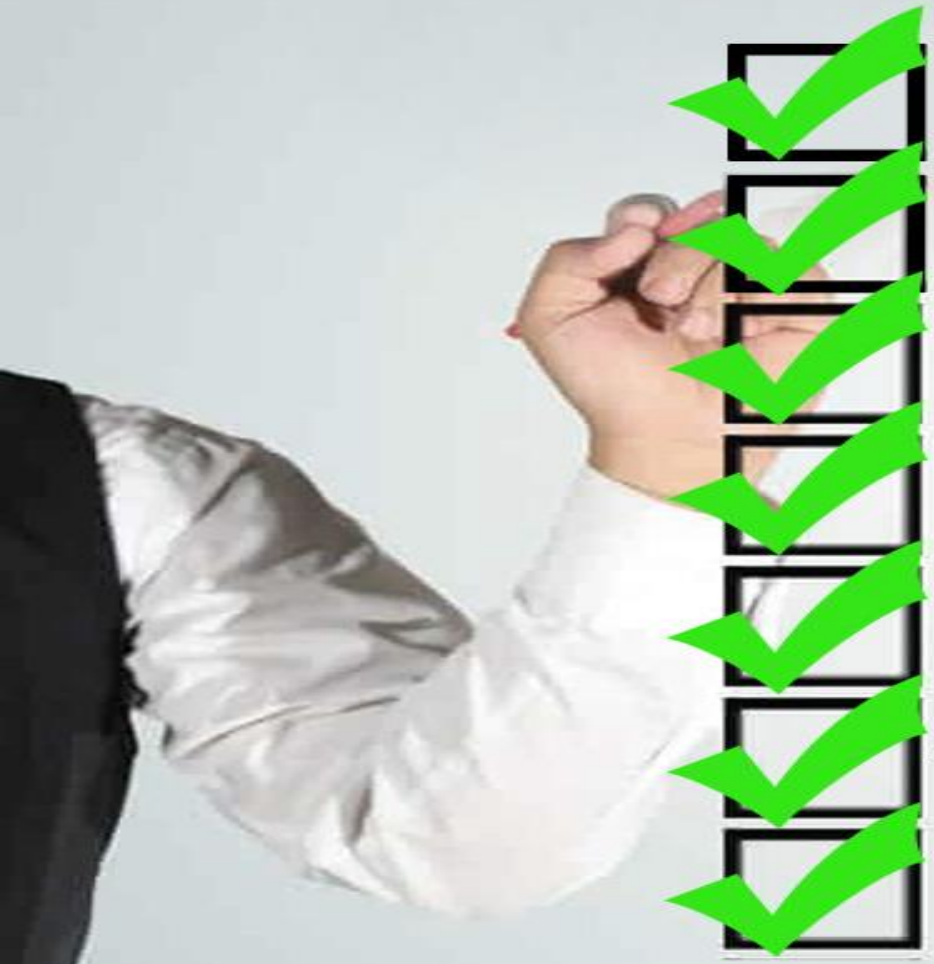


- Use strong passwords
- Set up two-factor authentication
- Use secure communication
- Set up firewalls
- Use an antivirus software
- **Secure your home router**
- Install updates regularly

EG|CERT

STAY SAFE .. WHILE WORKING AT HOME

أحمى جهازك .. اثناء عملك من المنزل



- Use strong passwords
- Set up two-factor authentication
- Use secure communication
- Set up firewalls
- Use an antivirus software
- Secure your home router
- Install updates regularly

EG | CERT

STAY SAFE..
WHILE WORKING AT HOME

كن أمن اثناء العمل من المنزل

Keep all software updated on devices connected to the Internet including computers,smartphones, and tablets to reduce the risk of malware.

حافظ على تحديث جميع البرامج على الأجهزة المتصلة بالأنترنت بما فى ذلك أجهزة الكمبيوتر و الهواتف الذكية و الأجهزة اللوحية لتقليل مخاطر البرامج الضارة.

EG | CERT

STAY SAFE WHILE WORKING AT HOME

أحمى جهازك..اثناء عملك من المنزل

Set a strong password that contains more than 12 characters with at least ONE CAPITAL character, ONE NUMBER & ONE SYMBOL. DON'T Forget to change it at least every 90 days.

استخدم الاحرف الكبيرة والصغيرة والرموز والارقام فيما لا يقل عن ١٢ حرف ورمز ورقم بشكل عشوائي و بدون تسلسل يسهل تخمينة.

EG | CERT

Stay Safe..
While Working
At Home

Use secure communication
استخدم اتصال مؤمّن

A secure communication tool assures that all of your internet traffic is encrypted, so it becomes less susceptible to eavesdropping or illegal interception, using a secure connection while working remotely makes your work related data much more safer.

تضمن أداة الاتصال الآمن أن كل حركة البيانات على الإنترنت الخاصة بك مشفرة مما يجعلها أقل عُرضه للتنصُت و الإعتراض الغير قانوني, لذلك فإن استخدام الإتصال المؤمن أثناء العمل عن بُعد يزيد من درجة حماية بيانات العمل.

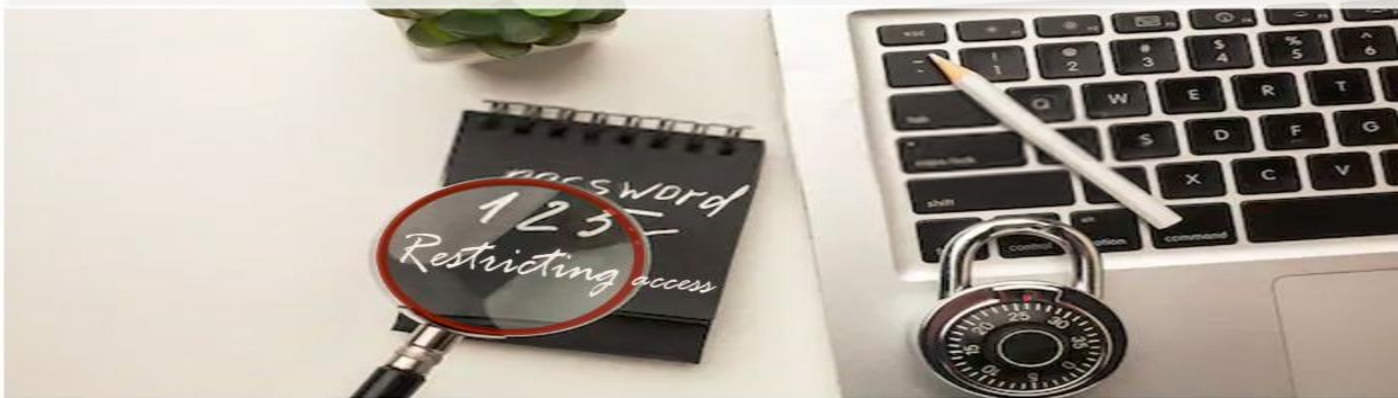
EG | CERT

Stay Safe..
While Working
At Home

أحمى جهازك..اثناء عملك من المنزل

Restricting access to the work device
استخدام جهاز العمل الخاص بك

- Only an authorized user should use the device, family and friends should not use a device released from work.
- يقتصر استخدام أجهزة العمل عليك وحدك أو على الأشخاص المسموح لهم بذلك , بحيث يجب ألا تستخدم العائلة والأصدقاء جهاز العمل الخاص بك.



EG | CERT

Stay Safe..
While Working
At Home

أحمى جهازك..اثناء عملك من المنزل

Use Log Off

استخدم خاصية تسجيل الخروج

- Always remember to **log off** your computer after finishing to protect your data.
- Better to set your device to lock automatically.

- تذكر دوما أن تقوم بتسجيل **الخروج** عند الإنتهاء من استخدام جهازك وذلك لكي تحمي بياناتك و ملفاتك الهامه.
- من الأفضل تفعيل خاصية إغلاق شاشة الجهاز التلقائي.

EG | CERT

DELTA PHARMA

PHARAONIA
PHARMACEUTICALS

التصيد الالكتروني

EG|CERT

التصيد الإلكتروني

هو أحد الهجمات السيبرانية التي تتم من خلال انتحال صفة شخص أو جهة موثوق فيها وذلك لجمع معلومات شخصية حساسة مثل بيانات البطاقات الإئتمانية أو كلمات المرور الخاصة و يكون ذلك عن طريق وسائل التواصل الإلكترونية كالبريد الإلكتروني و الرسائل النصية و المكالمات و وسائل التواصل الاجتماعي.

EG|CERT

كيف تأمن نفسك على مواقع المحادثات العامة

«الدردشة»

١ استخدم **اسم مستعار أو لقب** بدل من اسمك الحقيقي

٢ لا تعطى أحد **معلوماتك الشخصية** هذه معلومات سرية

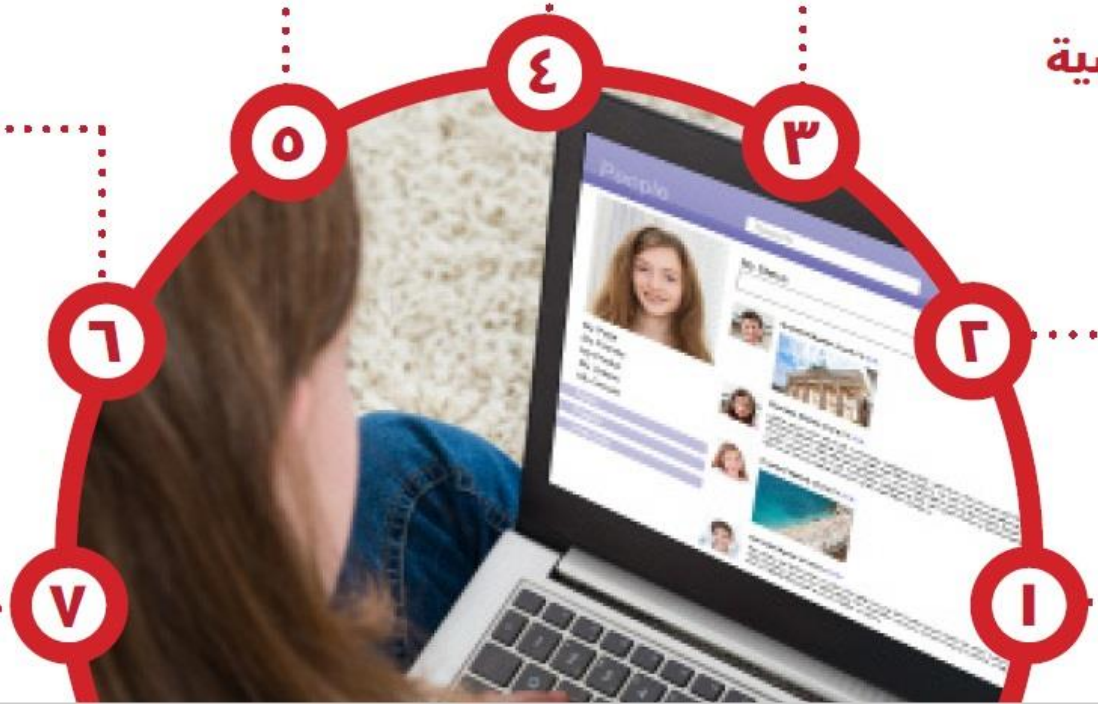
٣ تجنب نشر **صور خاصة** لك

٤ عند استخدام جهاز كمبيوتر عام، **ادخل** اسم المستخدم وكلمة المرور **يدويًا**

٥ تجنب مقابلة **الأشخاص الغرباء** الذين قابلتهم عبر الإنترنت

٦ افتح أو حمل فقط **ملفات معلومة المصدر**

٧ يفضل البقاء في **غرف الدردشة العامة** تجنب غرف الدردشة الخاصة



لا تقع ضحية للنصب و الابتزاز الإلكتروني بسبب فيروس كورونا

١

لا تفتح اى إيميل مجهول الهوية فقط لان مكتوب عليه نصائح لتجنب فيروس كورونا .

٢

لا تتبرع لاى جهة غير موثوق فيها فقط لانها تحثك على التبرع لصالح علاج فيروس كورونا.

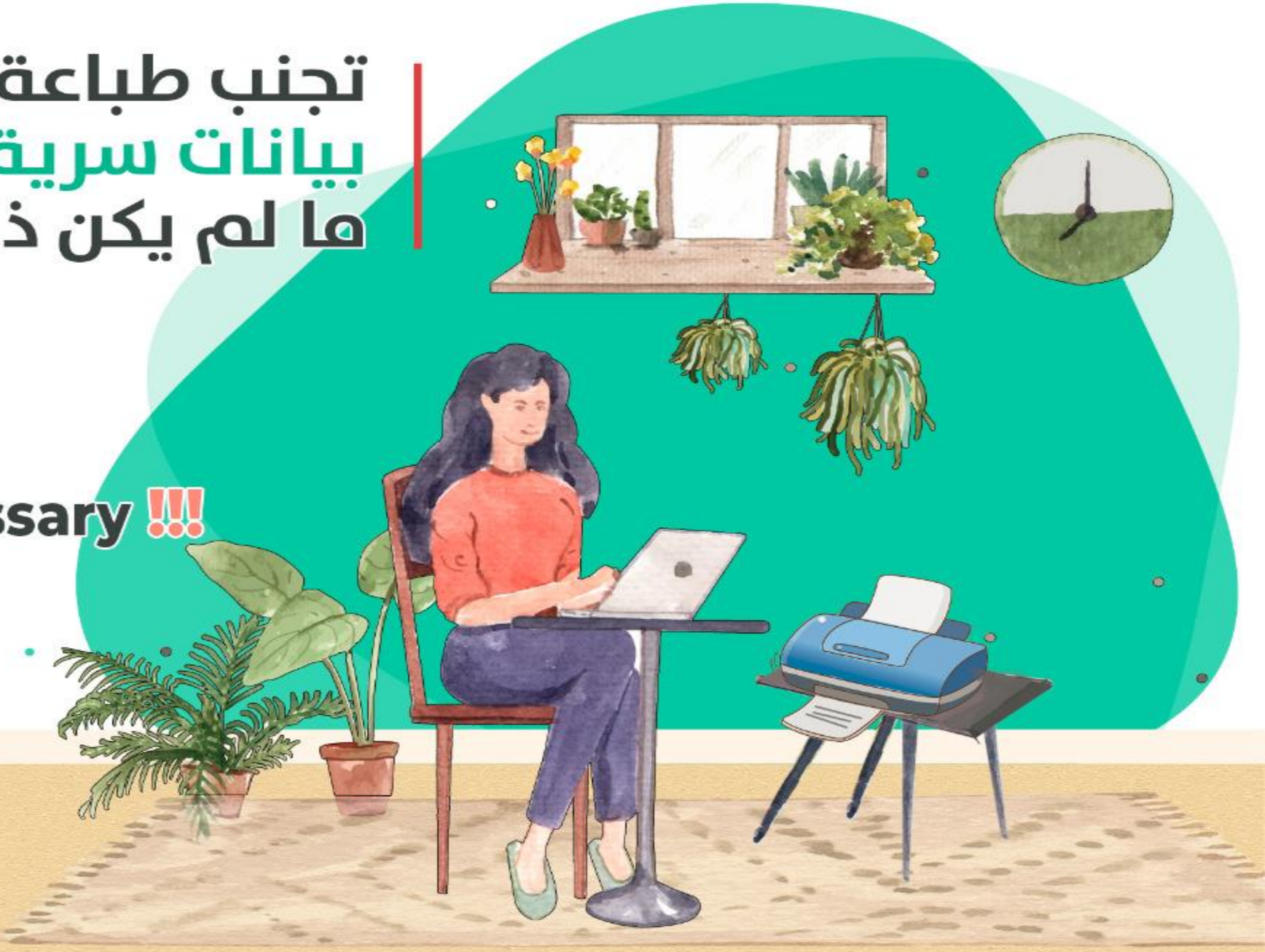
٣

لا تكون عرضة للابتزاز الإلكتروني, **لا** تثق فى أشخاص لا تعرفها و ترسل لهم بيانات شخصية او صورك **ولا** تفتح اى روابط او ملفات مرسله منهم.

EG|CERT

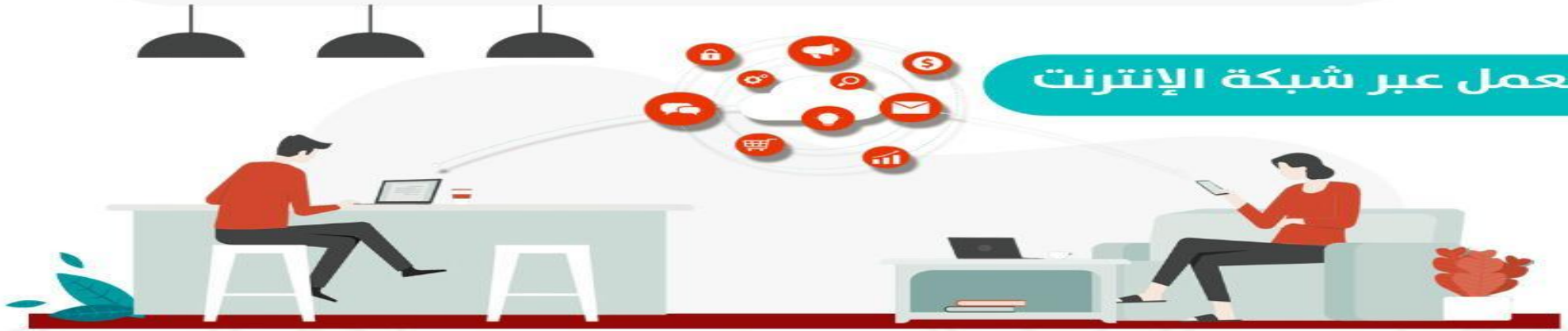
تجنب طباعة
بيانات سرية و مهمة
ما لم يكن ذلك ضروريا !!!

Avoid printing
sensitive data
unless it is necessary !!!



EG CERT

كيفية تأمين العمل عن بعد



قم دائما بفحص الملفات
باستخدام برنامج محدث لمكافحة البرمجيات الخبيثة قبل أن تشاركها مع أحد.

لا تقم بفتح أو مشاركة ملفات
واردة من مصادر غير معلومة مع الآخرين.

لا تقبل أي دعوات من مستخدمين
غير معروفين.

قم بالإبلاغ فورًا عن أي نشاط
مريب لمسؤول النظام الخاص بك.

لا تقم بتسجيل أي محادثة
أو أخذ لقطة شاشة منها بدون الحصول على إذن جميع الأطراف.

EG | CERT

يتعرض الكثير من مستخدمي الإنترنت لعمليات سرقة و تخريب بيانات عن طريق برمجيات خبيثة ، فما هي تلك البرمجيات الخبيثة؟؟ و كيف تعمل؟؟

البرمجيات الخبيثة: Malware

برمجيات يتم من خلالها إختراق أنظمة الكمبيوتر الخاصة بالأفراد أو المؤسسات الحكومية و المالية و الخدمية بدون علم تلك المؤسسات لأغراض ضارة مثل تعطيل الخدمة، سرقة البيانات و المعلومات الحساسة، تشفير الملفات بغرض الإبتزاز،و التحكم عن بعد في أنظمة الكمبيوتر الخاصة بتلك الجهات.

أشهر أنواع البرمجيات الخبيثة:

فيروس الحاسوب: Virus

برنامج خبيث يرتبط ببرنامج آخر عند تحميله ويكرر نفسه ليصيب برامج أخرى.

دودة الحاسوب : Worm

برمجيات خبيثة لديها القدرة على الانتشار تلقائياً من جهاز كمبيوتر لآخر بدون أي تدخل يدوي من المستخدم بهدف التحكم في الأجهزة.

فيروس الفدية: Ransomware

يقوم بتشفير ملفات المستخدم و طلب فدية لإستعادة الملفات.

فيروس الإعلانات المتسللة : Adware

فيروس يعمل في الخفاء لمعرفة إهتمامات المستخدم ومن ثم إرسال مواد دعائية وإعلانية تتوافق مع إهتماماته

برمجيات التجسس: Spyware

برمجيات تعمل في الخفاء وتقوم بسرقة المعلومات الخاصة من جهاز الكمبيوتر الخاص بالمستخدم مثل الرسائل و المحادثات و المستندات الخاصة.

حصان طروادة : Trojan

برمجيات خبيثة يتم دمجها داخل برامج سليمة لكي تخدع المستخدم لتثبيتها على نظامه بهدف اختراق الجهاز لأغراض ضارة.

راصد لوحة المفاتيح: Keylogger

برنامج يقوم بتسجيل ما يكتبه الشخص على جهازه حتى يتمكن المهاجم من معرفة كلمات السر و المعلومات الحساسة للمستخدم.

شبكة الروبوتات : Botnets

مجموعة من الأجهزة المصابة التي تكون في الغالب أجهزة غير محدثة أو ذات إعدادات تلقائية و كلمات سر ضعيفة يتحكم بها المهاجم و يستخدمها في هجمات أخرى مثل هجوم تعطيل الخدمة (DoS).

EG|CERT

أنواع البرمجيات الخبيثة

فيروس الحاسوب

فيروس الفدية

فيروس الإعلانات المتسللة

راصد لوحة المفاتيح

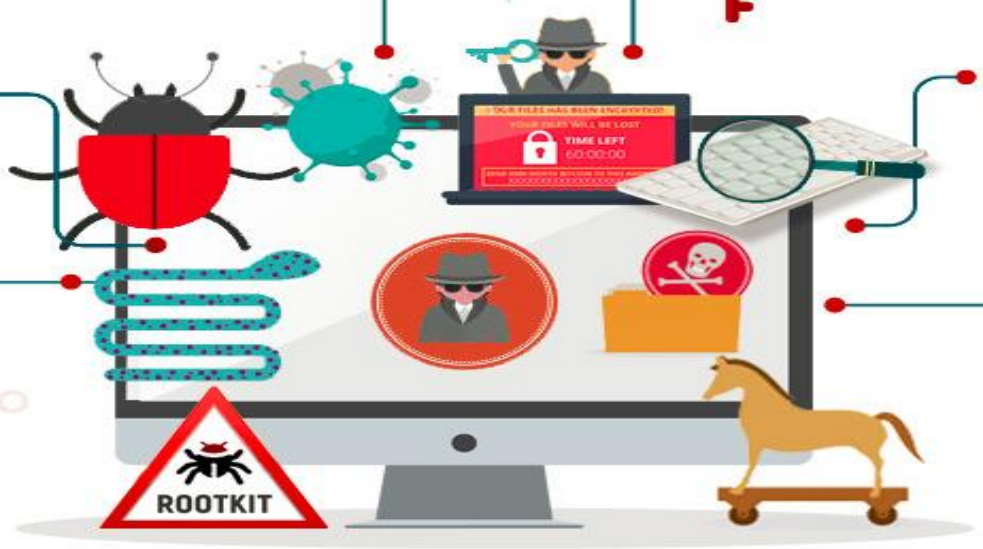
دودة الحاسوب

برمجيات الدخول عن بعد

برمجيات الجذور الخفية

حصان طروادة

برمجيات التجسس



EG|CERT

DELTA PHARMA

PHARAONIA
PHARMACEUTICALS

ولكم منا جزيل الشكر