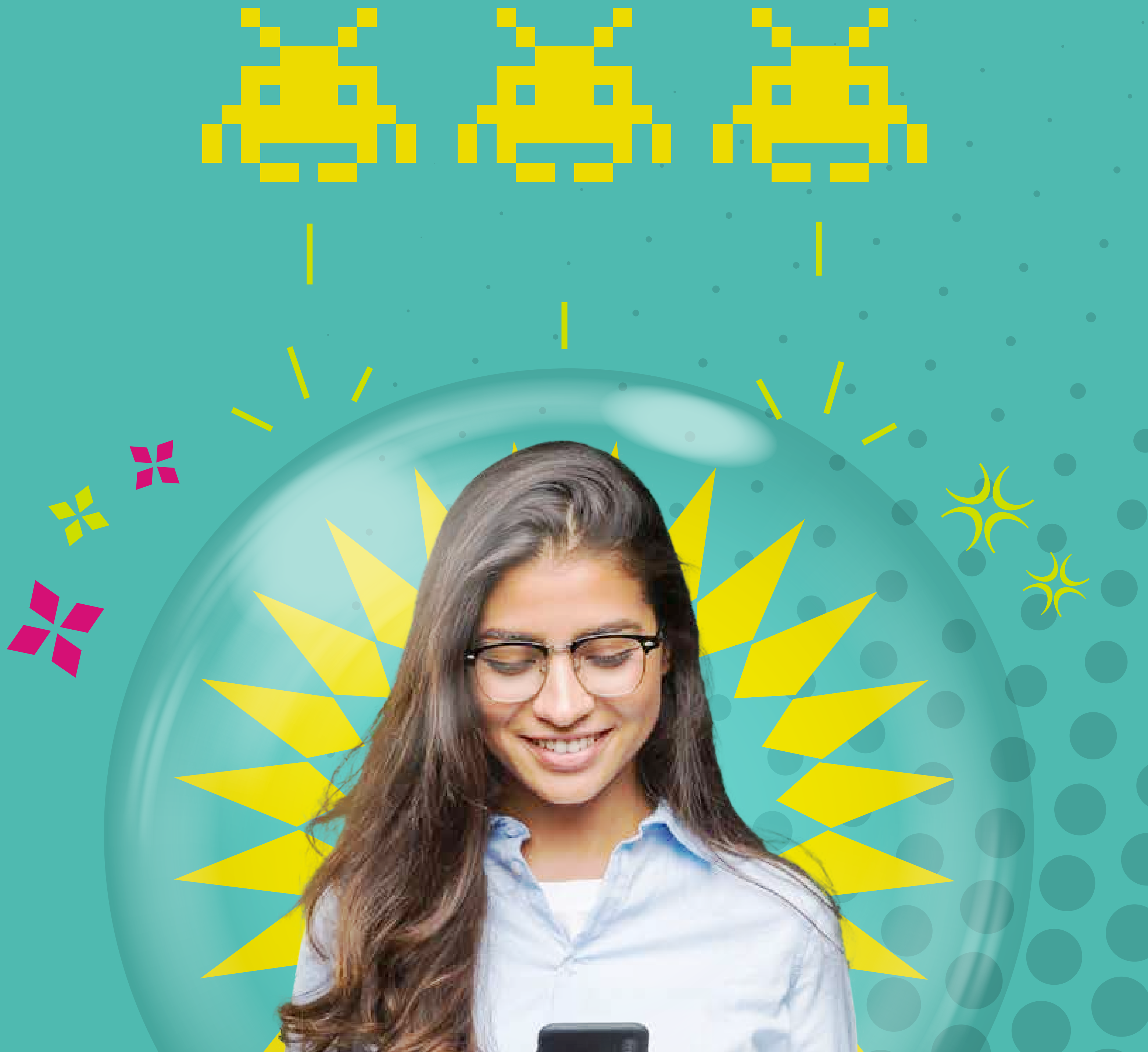
# Be Aware Be Secure

# حاسب. خلك آمن.



# TWO-FACTOR AUTHENTICATION

Two-factor authentication works with two separate security or validation mechanisms. Typically, one is a physical validation token, and one is a logical code or password. Both must be validated before accessing a secured service or product. This authentication method helps address the vulnerabilities of a standard password-only approach.

## What is two-factor authentication?

Supplementary passwords that provide an online account with a second layer of security

## How does two-factor authentication work?

It provides a way of proving a login is legitimate that's completely separate from the password.

## Why does two-factor authentication matter?

Adding two-factor authentication to an account makes it harder for a stolen password to be used against you.

## How safe is two-factor authentication?

The biggest risk is not technological; it is about social engineering, which can bypass even the most secure systems.

## How do I start using two-factor authentication

Enable two-factor authentication on your accounts by checking if a particular website offers the service.

# التحقق بخطوتين

يعمل التحقق بخطوتين على التحقق من صحة معلومات المستخدم باستخدام آليتين معاً: كلمة السر ورمز دخول مؤقت. عادةً ما يتم إنشاء الرمز بشكل فوري من خلال جهاز نقال. يجب التحقق من كليهما قبل الوصول إلى الخدمة. تساعد طريقة المصادقة هذه على معالجة الثغرات الأمنية التي تنشأ عن قرصنة كلمة السر.

## ما هو التحقق بخطوتين؟

إضافة طبقة إضافية من الأمان لعملية تسجيل الدخول من خلال إضافة إلى كلمة السر.

## كيف يعمل التحقق بخطوتين؟

يوفر طريقة لإثبات تسجيل الدخول منفصلة تماماً عن كلمة السر.

## لماذا تفعيل التحقق بخطوتين ضروري؟

يؤدي تفعيل التحقق بخطوتين إلى صعوبة اختراق الحساب حتى في حال كانت كلمة السر الخاصة بالحساب مسروقة.

## إلى أي مدى التحقق بخطوتين آمن؟

الخطر الأكبر ليس تكنولوجيا: إنها الهندسة الاجتماعية التي يمكنها اختراق الأنظمة الأكثر أماناً.

## كيف أبدأ في استخدام التحقق بخطوتين؟

فعل ميزة التحقق بخطوتين على حساباتك في المواقع الإلكترونية التي توفر هذه الميزة.

# BACKUP

Backup refers to the process of making copies of data or data files to use in the event where the original data or data files are lost or destroyed. Backups will be used to recover data after its loss from data deletion or corruption, or to recover data from an earlier time.

## Why you need to backup?

A computer or a smart phone is replaceable, your personal data is not.

## How to backup your files

Manual backup to USB, automatic backup to external hard drive, or cloud.

## How often should you backup?

Everyday or at least any time you make significant changes that you'd like to keep.

## Automation

Automate your backups as much as possible and check them regularly.

## Recovery

Backing up your data is only half the battle; you have to be certain that you can recover it.

# النسخ الاحتياطي

النسخ الاحتياطي هو عملية إنشاء نسخ من البيانات أو الملفات الهامة لاستخدامها في حالة فقدان أو إتلاف البيانات الأصلية. يتم استخدام النسخ الاحتياطية لاستعادة البيانات بعد فقدانها عن طريق الحذف أو تعطل الجهاز.

## لماذا تحتاج إلى النسخ الاحتياطي؟

الكمبيوتر أو الهاتف قابلان للاستبدال، بياناتك الشخصية ليست كذلك.

## كيفية النسخ الاحتياطي للملفات الخاصة بك

النسخ الاحتياطي اليدوي أو النسخ الاحتياطي التلقائي على قرص صلب خارجي أو عبر النسخ الاحتياطي السحابي.

## كم مرة يجب عليك النسخ الاحتياطي؟

كل يوم أو على الأقل في أي وقت تقوم بإجراء تغييرات كبيرة تريد الاحتفاظ بها.

## التشغيل الأوتوماتيكي

قم بالنسخ الاحتياطي بشكل تلقائي لبياناتك الخاصة إلى أقصى حد ممكن وتحقق منها بانتظام.

## الاسترداد

النسخ الاحتياطي للبيانات الخاصة بك هو نصف المشوار فقط، عليك أن تكون على يقين من أنه يمكنك استردادها عند الحاجة.

# CLOUD

Cloud computing is a type of computing that relies on shared computing resources rather than having local servers or personal devices to handle applications. Major threats to cloud security include data breaches, data loss, account hijacking, service traffic hijacking, poor choice of cloud storage providers, and shared technology that can compromise cloud security.

## Due Diligence

Remain informed on the latest security issues and strategies.

## Encryption

Double check that the cloud service provider encrypts data.

## Two-Factor Authentication

Use two-step authentication to log in to important accounts, such as sending a code via SMS in addition to the password.

## Storage

Routinely monitor workspaces and back up data to avoid data loss.

# تكنولوجيا الحوسبة السحابية

الحوسبة السحابية Cloud computing هي نوع من الحوسبة على موارد الحوسبة المشتركة بدلًا من وجود خوادم محلية أو أجهزة شخصية للتعامل مع البيانات والتطبيقات. تعتبر خروقات وفقدان البيانات وسرقة الحسابات والاختيار السيئ لموفري التخزين السحابي من أهم التهديدات الرئيسية التي يمكن أن تهدد أمن السحابة.

## الحرص واجب

اجعل نفسك مطلعاً على أحدث اتفاقية شروط وأحكام استخدام مزود الخدمة السحابية.

## التشفير

تحقق مرة أخرى من قيام مزود الخدمة السحابية بتشفير البيانات.

## التحقق بخطوتين

استخدم المصادقة المكونة من خطوتين لتسجيل الدخول إلى خدمات السحابة مثل استخدام رمز من خلال رسالة نصية بالإضافة إلى كلمة السر.

## التخزين

راقب بشكل روتيني مساحات العمل والنسخ الاحتياطية للبيانات لتجنب فقدان البيانات.

# MALWARE

Malware is defined as a software intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. It is mainly used to gain unauthorized access to systems and/or resources which may cause unauthorized disclosure of sensitive data, denial of service, unwarranted deletion, etc.

## Keep software up to date

Attackers know about weaknesses in the software on your device before you do.

## Don’t pay the ransom

You might get asked to pay repeatedly without any resolution.

## Data should be backed up frequently

No one ever thinks they will be hacked until they do.

# البرمجيات الخبيثة

يتم تعريف البرنامج الخبيث على أنه يهدف إلى تنفيذ عملية غير مصّرح بها ولها تأثير سلبي على أمن النظام أو كفاءته أو توفره. وتستخدم هذه البرامج بشكل أساسي للوصول غير المصّرح به إلى الأنظمة و/أو الموارد التي قد تتسبب في الكشف غير المصّرح به عن البيانات الحساسة، وعدم توفر الخدمة، والحذف وفقدان البيانات الهامة، إلخ.

### حافظ على تحديث البرامج

يعرف المهاجمون نقاط الضعف في البرامج على جهازك قبل معرفتك بذلك.

### لا تدفع أموالًا

قد يطلب منك الدفع مراراً وتكراراً من دون تقديم أي حل فعلي.

### قم بنسخ احتياطي للبيانات

لا أحد يعتقد أنه بالامكان اختراق بياناته حتى يقع ضحية للاختراق.

# MOBILE SECURITY

Mobile devices may contain sensitive personal information and data files that should be secured. Information security threats against mobile devices will cause exposure of sensitive information, installation of viruses and spywares, or the device could be lost  or stolen.

## Keep software up to date

Keep your software and operating systems up to date.

## Secure with a password

Use strong passwords. Always use lock screen features.
Enable Touch ID if it is available.

## Enable remote wiping

Activate the feature that allows you to track your phone remotely.
Ensure that it allows you to wipe all data from your device if it is lost or stolen.

## Enable device auto-lock

Always use auto-lock. Never share your password.

## Personal information is valuable

Protect it! Take care of your personal information; think about which apps you allow to access it. Check whether apps and websites are collecting too much data from you.

# أمن الهاتف

قد تحتوي الهواتف النقالة على معلومات شخصية حساسة وبيانات يجب تأمينها. قد تتسبب تهديدات أمن المعلومات ضد الهواتف النقالة بكشف وسرقة معلومات حساسة أو تثبيت الفيروسات وبرامج التجسس.

## حافظ على تحديث النظام

حافظ على تحديث برامجك وأنظمة التشغيل الخاصة بك.

## حماية الهاتف بكلمة سر

استخدم كلمات قوية. دائماً استخدم ميزات قفل الشاشة.

## فعّل ميزة ايجاد الهاتف في حال ضياعه

قم بتفعيل الميزة التي تتيح لك تعقب هاتفك عن بُعد. تأكد من أنه يسمح لك بمسح جميع البيانات من جهازك في حالة ضياعه أو سرقته.

## فعّل القفل التلقائي للجهاز

دائماً استخدم القفل التلقائي. لا تشارك كلمة السر مطلقاً.

## المعلومات الشخصية قيّمة

اعتن بمعلوماتك الشخصية. فكر قبل السماح للتطبيقات بالوصول إليها. تحقق مما إذا كانت التطبيقات ومواقع الويب تجمع الكثير من البيانات منك.

# PASSWORDS

## Change

Change passwords at regular intervals and avoid using the same passwords periodically and for multiple platforms.

## Complex

Use complex passwords which are at least 8 characters long with a combination of numbers and symbols.

## Default

Change the initial password immediately after the first log in.

## Don’t

Do not store passwords in insecure digital or physical form and do not share it with anyone.

## 2FA

Enable 2 Factor Authentication for all your corporate and personal accounts - along with passwords, also generate a mobile PIN.

# كلمة السر

## تغيير

غير كلمة السر على فترات منتظمة وتجنب استخدام كلمات السر نفسها بشكل دوري ولعدة مواقع إلكترونية.

## صعبة

استخدم كلمة سر معقدة تتكون من ٨ أحرف على الأقل مع مجموعة من الأرقام والرموز.

## الإعدادات الافتراضية

غيّر كلمة المرور الأوّلية مباشرة بعد تسجيل الدخول الأول.

## لا تقم

لا تقم بتخزين كلمات السر بشكل رقمي أو على ورقة ولا تشاركها مع أي شخص.

## التحقق بخطوتين

فعل ميزة التحقق بخطوتين لجميع حساباتك - إلى جانب كلمة السر، خصص ايضاً رقم تعريف من الهاتف النقال.

# RANSOMWARE

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware authors order that payment  be sent via cryptocurrency or credit card. Ransomware typically spreads through phishing  emails or by unknowingly visiting an infected website.

## Backup is always a good idea

Backup is the best way to protect your data. You do not have to back up everything, the most important files are enough.

## Install Updates

Having an up-to-date system and software means having the best possible versions of these at the time.

## Be Careful Online

The best way to stay safe is to develop kind of a gut feeling what is right and what is wrong online.

## Anti-Ransomware

One of the methods to prevent ransomware attack is to install special anti-ransomware tools.

# برامج دفع الفدية

برنامج دفع الفدية Ransomware هو نوع من البرامج الضارة، المصممة لمنع الوصول إلى بياناتك الهامة حتى يتم الدفع لفك المنع. عادةً يطلب مطوروا هذه البرامج دفع مبالغ عبر عملة مشفرة مثل بيتكوين Bitcoin أو بطاقة الائتمان. تنتشر برامج دفع الفدية عادةً من خلال رسائل البريد الإلكتروني للتصيّد أو عن طريق زيارة موقع ويب ملغّم بهذه البرامج بدون معرفة مسبقة.

## النسخ الاحتياطي

أفضل طريقة لحماية البيانات الخاصة بك هي أخذ نسخ احتياطية. ليس عليك القيام بنسخة احتياطية لكل شيء. فقط للملفات الأكثر أهمية.

## تثبيت التحديثات

وجود نظام وبرامج محدثة يعني وجود أفضل الإصدارات المتوفرة منها (أمنياً) في هذا الوقت.

## كن حذراً على الانترنت

أفضل طريقة للبقاء في أمان هي تطوير نوع من الشعور بالمسؤولية حول ما تقوم به على الأنترنت.

## مكافحة برامج دفع الفدية

إحدى الطرق لمنع هجوم برامج الفدية هي تثبيت أدوات خاصة لمكافحة هذا النوع من البرامج.

# SOCIAL ENGINEERING

Social engineering is the art of manipulating people so they give up confidential information. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. Security is all about knowing who and what to trust.

## Spotting A Phishing Email

- Spelling errors (e.g., "pasword"), lack of punctuation or poor grammar.
- Hyperlinked URL differs from the title name displayed, the link is shortened. Always hover over the link to get more details.
- Sense of urgency. Phishing emails will usually use a language that demands for immediate actions.
- Personally identifiable information. Requests for personal information like credentials or financial information.
- Suspicious attachment. Request to open attachments to check and verify data.

# الهندسة الاجتماعية

الهندسة الاجتماعية هي فن التعامل مع الأشخاص واستدراجهم للكشف عن معلومات سرّية. يستخدم المجرمون أساليب الهندسة الاجتماعية لأنه عادة ما يكون من الأسهل استغلال ثقة الأشخاص من اكتشاف طرق فنية لاختراق الأنظمة الخاصة ومعرفة من تثق بـه.

## اكتشاف رسالة بريد إلكتروني للتصيد الاحتيالي

- الأخطاء الإملائية، أو عدم وجود علامات ترقيم أو قواعد نحوية ضعيفة.
- رابط تشعبي مختلف عن اسم العنوان المعروض، والرابط قصير. قم دائماً بالمرور فوق الرابط للحصول على مزيد من التفاصيل.
- عادةً ما تصاغ رسائل البريد الإلكتروني المخادعة بإسلوب يدعو إلى إجراءات فورية.
- عادة ما تحتوي الرسائل المخادعة طلبات للحصول على معلومات شخصية مثل بيانات الاعتماد أو المعلومات المالية.
- تحتوي الرسائل المخادعة في الغالب على طلب فتح مرفقات للفحص والتحقق من البيانات.

# SOCIAL MEDIA

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, and wikis are among the different types of social media.

CyberBOTs constantly keep their ears to the internet and listen for people who are disclosing company information or working for companies they are targeting for information sharing.

## Information Sharing

- Never post company information over social networks.
- Persists. Whatever you write on the internet is written in ink, not pencil.
- Malicious links often come from friends' compromised accounts. Be cautious of offers that are too good to be true and lead to strange websites.

# وسائل التواصل الاجتماعي

وسائل التواصل الاجتماعي هي مجموعة من قنوات الاتصال عبر الإنترنت مخصصة للمداخلات الاجتماعية والتفاعل ومشاركة المحتوى والتعاون. تعد المواقع والتطبيقات المخصصة للتواصل والتدوين المصغر والمشاركة والشبكات الاجتماعية من بين الأنواع المختلفة لوسائل التواصل الاجتماعي.

يبقي الجواسيس والقراصنة آذانهم صاغية عبر الإنترنت بحيث يستمعون للأشخاص الذين يكشفون عن معلومات الشركة التي يعملون لصالحها مما يساعدهم على استهدافها.

### مشاركة المعلومات

- لا تنشر معلومات عن الشركة الخاصة بك دون وجود إذن مسبق.
- يبقى للأبد. كل ما تكتبه على الإنترنت مكتوب بالحبر وليس بقلم الرصاص.
- غالباً ما تأتي الروابط الضارة من حسابات الأصدقاء المخترقة. توخى الحذر من العروض التي تكون جيدة للغاية بحيث لا يمكن أن تكون حقيقية وتؤدي إلى مواقع مريبة.