



OCTOBER | CYBERSECURITY MONTH

Cyber threats in the workplace: how to identify them and minimise their impact

A digital environment with more exposure points

Businesses rely on **more applications, cloud services, devices, and digital identities**. Every connection makes work easier, but it can also open up a vulnerability if not managed properly.

The familiar methods are still in use: deceiving a person, exploiting a vulnerability or using a compromised account. What has changed is the **ability to combine techniques, automate attacks and create more convincing messages with the help of AI**. Therefore, protecting yourself requires an understanding of both the methods of access and their potential consequences.

Warning signs in your digital environment



A request that breaks the routine

Someone urgently requests a transfer, a password or a change to payment details.



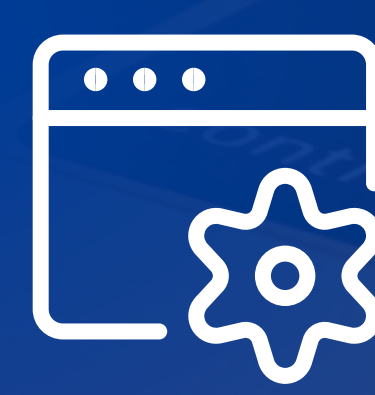
Access you do not recognise

A login attempt, a new device or unexpected activity appears on an account.



A service that behaves differently

An app stops responding, becomes very slow or files are no longer available.



A system left exposed without up-to-date protection

There are unsupported applications, pending patches or internet accessible services that are not being monitored.

These signs do not, on their own, identify the type of attack. Nor do some threats give obvious warning signs before an incident occurs. The key is to check for anomalies and report them in good time.

The 5 cyber threats your business needs to be aware of

01

Phishing and social engineering



- **What exactly is it?**

An attacker impersonates a trusted person or organisation to obtain information, access or a payment.

- **¿Cómo suele manifestarse?**

An email asking you to open an invoice, a text message containing a link, or a phone call requesting an urgent bank transfer. It may arrive via a familiar channel and appear convincing.

- **¿Cómo suele manifestarse?**

Verify any unexpected requests via a different channel from the one used to contact you. Access services via their official websites.

02

Vulnerability exploitation



- **What exactly is it?**

A flaw in an application, device or system is exploited to gain access to it or carry out unauthorised actions.

- **How does it usually manifest itself?**

A service accessible through the internet remains unupdated or uses a version that is no longer supported. It is not necessary for a person to open a suspicious message.

- **¿Cómo suele manifestarse?**

Identify exposed assets and prioritise fixing flaws that affect critical services or are already being exploited.

03

Credential theft



- **What exactly is it?**

A compromised password, session or other access data allows the attacker to log in as if they were a legitimate user.

- **How does it usually manifest itself?**

Logins from unknown devices or unusual activity are detected. Credentials may result from a phishing attack, a data breach or malicious software.

- **What should you do?**

Enable multi-factor authentication, avoid reusing passwords, limit permissions and review login alerts.

04

Ransomware



- **What exactly is it?**

Attackers encrypt systems or steal information in order to demand a payment. The incident may compromise data and bring operations to a standstill.

- **How does it usually manifest itself?**

Inaccessible files, disrupted systems or threats to publish information. Initial access may have been gained previously via a compromised account or a vulnerability.

- **What should you do?**

Protect and test backups, limit the spread between systems, and practise your response and recovery procedures.

05

DDoS attacks



- **What exactly is it?**

Multiple sources send traffic or requests to overload a website, application or digital service.

- **How does it usually manifest itself?**

The service responds very slowly or becomes unavailable to many users at once. The attacker may seek to disrupt the service without accessing the data.

- **¿Cómo suele manifestarse?**

Put mitigation measures in place with your service providers and define how to maintain or restore essential services.



AI also fuels attacks

Attackers can use it to automate tasks, personalise campaigns and create more convincing fake messages, voices or videos. When faced with a request for access, sensitive information or money, verify the identity via an independent channel, even if it appears genuine.

Why Telefónica Tech?

At Telefónica, we have taken on the clear challenge of becoming the best gateway for citizens, businesses, and institutions to access digital technologies.

We combine **cybersecurity specialists with managed services** to protect identities, identify vulnerabilities and detect and respond to incidents.

We help you prioritise risks and take action to minimise the impact on your business through our **Digital Operations Centre** and our global network of **SOCs**.

