CYBERATTACKS SCRIPT

Hi! Are you one of those people who hide your credit card code when you pay? And... are you also one of those people who has covered over the webcam on your computer? Yes? Congratulations, these are very important things to do.

But, why do you then open emails from unknown senders? Whether you are an individual or on your company's corporate network, you should be on your guard because at any moment you could get a nasty visit... from a hacker.

The podcast for everyone who wants to change the world. Now is the time to think about the future of the planet. What do need to know about... cyberattacks?

(*introduction*)

In the 21st century, the century of digitalisation, technology is evolving in leaps and bounds. But the advances in artificial intelligence, big data and Industry 4.0 also have their downsides. The internet is vulnerable, and cyberattacks threaten the information held by individuals, companies and entire countries. In fact, in the words of technology policy and digital development expert Alec Ross:

https://www.iberdrola.com/shapes/alec-ross-ciberconflictos-que-definiran-los-proximos-cinco-anos

The increasing extent of cybercrime is incurring spectacular costs. By 2021, the total cost of cybercrime is expected to reach $6 billion. This figure will increase to more than $10 billion by 2025, making cybercrime one of the biggest issues and challenges for business and society in the coming years.

So, what exactly are cyberattacks, and how have they affected human progress?

(*sound of typing, wrong password)*

A cyberattack is a series of actions targeting information systems, such as databases, with the aim of harming individuals and organisations. The aim is to disable services, spy on competitors' activities, steal information and even extort money from an institution.

Spying and information theft is intrinsic to human existence. From anticipating enemy invasions to a virus placed on the server of a leading multinational, there have been countless attacks on modern communication systems.

(*time machine/time travel sound, inquisitive tone) Year 1940-1942*
The most famous enigma of the Second World War was deciphered by the mathematician Turing, who by creating the "Bombe" machine deciphered the Enigma code, the secret code used by the Germans. Breaking this code helped the Allies win the war.

(*time machine/time travel sound, inquisitive tone)* Year 1834
But the first known cyberattack involved the optical telegraph, a novel communication system used by the French government. Until the Blanc brothers arrived on the scene.

These two bankers wanted to take advantage of the system to be the first to know the situation on the French market, which took several days to arrive from the country's capital. They bribed a technician who hid the value of French bonds among the government's messages, which were instantly intercepted by an assistant of the brothers. This cyberattack lasted more than two years.

(*time machine/time travel sound, inquisitive tone)* Decade 2010

In recent years, cyberattacks have left their mark on a large scale, generating economic conflict and social panic.

In 2008, a worm infiltrated vulnerable Windows systems, infecting 10 million computers in 190 countries. In 2010, Iran and other countries feared a nuclear attack following a breach of critical infrastructure. And in 2017, a large number of computers in Europe had their files encrypted and access to them blocked. Thousands of businesses were paralysed by a very descriptive malware called "wannacry".

(*time machine/time travel sound, inquisitive tone)* Year 2021

Today we are more likely to experience cyberwarfare than traditional warfare, as Keren Elazari, a cyber security and hacker culture specialist with several TED talks under her belt, points out.

https://www.iberdrola.com/shapes/keren-elazari-ciberguerra-en-el-contexto-de-los-conflictos-mundiales

In the age of cyberwarfare, countries and companies alike have redrawn the battle lines to make them virtual. This era began about ten years ago, when a computer virus called Stuxnet changed the rules of the game. It was the world's first cyberweapon: a computer code capable of altering physical facilities. In the context of geopolitics, a digital weapon such as Stuxnet could simply be understood as the most practical, non-violent and cost-effective means of covertly disrupting a nuclear weapons programme.

And many criminal organisations now use cyberattacks. In fact, during the pandemic, their activity increased by 25%. Their high profitability and the difficulty of tracing them make them very attractive to hackers.

(explanatory and enumerative)
There are several types of cyberattack, depending on how they are carried out, their purpose, their victim...

(in an aside) Let's find out about them with Kaspersky, a leading cybersecurity company.

- Phishing. Sending fraudulent messages that appear to come from reliable and secure sources. Most commonly used in email. The aim is to steal personal data such as passwords or banking information.
- Malware. Malicious software with viruses or worms. Their impact ranges from installing harmful software to blocking access to network components (ransomware) or obtaining information (spyware).
- SQL injection. A hacker inserts malicious code into a server using structured query language, revealing protected information.
- Denial of service attack. It saturates systems, servers and even networks with traffic to exhaust their resources and bandwidth.

(explanatory)

To protect yourself from these cyberattacks you need a cyberattack security network. This system quickly detects, identifies and stops threats, creating a security perimeter. It controls who enters your network, and protects all devices linked to your network, both at home and at work.

(*enumerated and practical, sound effects related to each item*)

But you can also help prevent these attacks in your everyday online life:

- Update your hardware and anti-virus software. The latest enhancements fix security flaws from previous versions.
- Use long and complex passwords. They should not always be the same or include easily decipherable information, such as your birthday or your pet's name.
- Do not click on suspicious links. Internet servers often warn of unsafe sites.
- Do not provide personal data to unknown or unreliable websites. Only trust safe and official spaces.
- Report any dubious websites, links or emails to the authorities.

Cyberattacks are advancing faster than technology and digitalisation itself. Although their detection is in the hands of national and international bodies, it is up to us to make it as difficult as possible by being smart users of the network of networks.

Thank you for caring about the future. Now it's time for action. Discover more inspiring initiatives for the planet in the following podcast, on your favourite listening platform, or in the innovation and sustainability sections at Iberdrola.com.