Watch the video about cybercrime and decide if the sentences are true or false.

1. Right now, every second, eight new users are joining the Internet.
2. Mostly you get infected with a computer virus because you went to a porn site.
3. Short-term-to-long-term DDOS service or scheduled attack costs 5 to 50 dollars per hour.
4. The Black Hole Exploit Pack is responsible for nearly one quarter of malware distribution in the last couple of quarters.
5. There are many ways you can get infected.
6. Hackers can turn on the webcam if we have a malware on our PC.
7. These days malware is mostly spread by writing scripts in not properly protected websites.
8. Cybersecurity specialists often track and find hackers.
9. About 16 percent of the profile pictures on Internet dating sites contain the GPS coordinates of where the photo was taken.
10. Mentioned by James Lyne cybercriminal was selling sphynx kittens.
11. Your smartphone is beaming out a list of networks you've previously connected to, only when you're using wireless actively.
12. “CIASurveillanceVan” wifi name was created for CIA intervention.
13. 2 % of audience had a tendency to utmost vulgarity.
14. Fewer and fewer people aren’t interested in the basics of how the technology works.
15. The cybercriminals James Lyne talked about, still haven't been arrested.
16. 99 percent of malware works because people fail to do the basics.
17. James Lyne claims that one of the best practice to protect our data is to use antiviruses.

Read the article and answer the questions:

1. Who and how came up with the word “hack”?

2. What was the first generation of hackers’ nickname and what have they discovered?

3. What was the story behind John Draper’s nickname?

4. What was the “blue box” and who got inspired by it?

5. What “hacking stuff” inquisitive kids from 1980s generation did?

6. Who was 414s and what they did?

7. What was the name of earliest version of the Internet and why it got jammed in 1988?

8. What L0pht testified before congress?

9. Why Microsoft offered bounty on hackers attacking Microsoft?

10. Who released Stuxnet virus and how it worked?

Solve a quiz.

1. What is the first device presented in the television?
    a. lawn mover b. snowblower c. teapot
2. How easy was breaking in into the computer system of Los Alamos National Laboratory?
    a. very easy b. very, very easy c. not very easy
3. What is young Timothy Winslow doing on the second picture?
    a. playing underwater chess
    b. riding a horse
    c. sitting on a bike
4. What emotion Neal Patrick express when his daughter starts frame 1.
    a. LOL b. LMAO c. ROTFL
5. What number on the phone choose an actor?
    a. 8
    b. 0 700
    c. who cares
6. “The 414s” name was created because they followed the example of:
    a. Milwaukee gangs
    b. Football teams
    c. Comic book super heroes
7. What movie was the inspiration for 414s?
    a. War games
    b. Star wars
    c. Saw
8. In which state is placed Los Alamos?
    a. Alaska
    b. New Mexico
    c. New York
9. Whose sister said “The FBI is here”?
    a. Timothy Winslow
    b. Neal Patrick
    c. the third guy with mustache
10. The media exaggerated the damage they caused by saying things like:
    a. they were causing sb to die
    b. they caused a fire because the system failed
    c. they had damaged all the data in the system monitoring the conditions of cancer patients
11. Who was Matthew Broderick that Neal Patrick was compared to?
    a. jewish actor
    b. well known hacker
    c. comic
12. As you may noticed all 3 characters introduced in this movie were friends at the beginning and later their lifes become more and more complicated because of FBI and media - which became the part of Neal life. Did this split 3 happy friends?
    a. yes
    b. no
    c. tldr;

The Evolution Of Hacking

Computer hacking was once the realm of curious teenagers. It's now the arena of government spies, professional thieves and soldiers of fortune.

Today, it's all about the money. That's why Chinese hackers broke into Lockheed Martin and stole the blueprints to the trillion-dollar F-35 fighter jet. It's also why Russian hackers have sneaked into Western oil and gas companies for years.

And think of the immense (and yet undisclosed) damage from North Korea's cyberattack on Sony Pictures last year. Computers were destroyed, executives' embarrassing emails were exposed, and the entire movie studio was thrown into chaos.

It wasn't always this way. Hacking actually has some pretty innocent and harmless beginnings.

Curiosity created the hacker

The whole concept of "hacking" sprouted from the Massachusetts Institute of Technology nearly 50 years ago. Computer science students there borrowed the term from a group of model train enthusiasts who "hacked" electric train tracks and switches in 1969 to improve performance.

These new hackers were already figuring out how to alter computer software and hardware to speed it up, even as the scientists at AT&T Bell Labs were developing UNIX, one of the world's first major operating systems.

Hacking became the art of figuring out unique solutions. It takes an insatiable curiosity about how things work; hackers wanted to make technology work better, or differently. They were not inherently good or bad, just clever.

In that sense, the first generation of true hackers were "phreakers," a bunch of American punks who toyed with the nation's telephone system. In 1971, they discovered that if you whistle at a certain high-pitched tone, 2600-hertz, you could access AT&T's long-distance switching system.

They would make international phone calls, just for the fun of it, to explore how the telephone network was set up.

This was low-fi stuff. The most famous phreaker, John Draper (aka "Cap'n Crunch) earned his nickname because he realized the toy whistle given away in cereal boxes emitted just the right tone. This trained engineer took that concept to the next level by building a custom "blue box" to make those free calls.

This surreptitious little box was such a novel idea that young engineers Steve Wozniak and Steve Jobs started building and selling it themselves. These are the guys who would later go on to start Apple.

Wire fraud spiked, and the FBI cracked down on phreakers and their blue boxes. The laws didn't quite fit, though. Kids were charged with making harassing phone calls and the like. But federal agents couldn't halt this phenomenon.

A new wave of hackers

The next generation came in the early 1980s, as people bought personal computers for their homes and hooked them up to the telephone network. The Web wasn't yet alive, but computers could still talk to one another.

This was the golden age of hacking. These curious kids tapped into whatever computer system they could find just to explore. Some broke into computer networks at companies. Others told printers at hospitals hundreds of miles away to just spit out paper. And the first digital hangouts came into being. Hackers met on text-only bulletin board systems to talk about phreaking, share computer passwords and tips.

The 1983 movie "War Games" depicted this very thing, only the implications were disastrous. In it, a teenager in Washington state accidentally taps into a military computer and nearly brings the world to nuclear war. It's no surprise, then, that the FBI was on high alert that year, and arrested six teenagers in Milwaukee -- who called themselves the 414s, after their area code -- when they tapped into the Los Alamos National Laboratory, a nuclear weapon research facility.

Nationwide fears led the U.S. Congress to pass the Computer Fraud and Abuse Act in 1986. Breaking into computer systems was now a crime of its own.

The damage of hacking started getting more serious, too. In 1988, the government's ARPAnet, the earliest version of the Internet, got jammed when a Cornell University graduate student, curious about the network's size, created a self-replicating software worm that multiplied too quickly.

The cat-and-mouse game between law enforcement and hackers continued throughout the 1990s. But hacks were still more of an annoyance than anything devastating, though it was quickly becoming apparent that the potential was there. The stock market, hospitals, credit card transactions -- everything was running on computers now. There was a bone-chilling moment when a ragtag group of hackers calling themselves L0pht testified before Congress in 1998 and said they could shut down the Internet in 30 minutes.

The danger was suddenly more real than ever.

From curiosity to criminal

The ethos was starting to change, too. Previously, hackers broke into computers and networks because they were curious and those tools were inaccessible. The Web changed that, putting all that stuff at everyone's fingertips. Money became the driving force behind hacks, said C. Thomas, a member of L0pht who is known internationally as the hacker "Space Rogue."

An unpatched bug in Windows could let a hacker enter a bank, or a foreign government office. Mafias and governments were willing to pay top dollar for this entry point. A totally different kind of black market started to grow.

The best proof came in 2003, when Microsoft started offering a $5 million bounty on hackers attacking Windows. "It's no longer a quest for information and knowledge by exploring networks. It's about dollars," Thomas said. "Researchers are no longer motivated to get stuff fixed. Now, they say, 'I'm going to go looking for bugs to get a paycheck - and sell this bug to a government.' "

Loosely affiliated amateurs were replaced by well-paid, trained professionals. By the mid-2000s, hacking belonged to organized crime, governments and hacktivists.

First, crime: Hackers around the world wrote malicious software (malware) to hijack tens of thousands of computers, using their processing power to generate spam. They wrote banking trojans to steal website login credentials.

Then there's government. When the United States wanted to sabotage the Iranian nuclear program in 2009, it hacked a development facility and unleashed the most dangerous computer virus the world has ever seen. Stuxnet caused the Iranian lab computers to spin centrifuges out of control.

Similarly, there's proof that Russia used hackers to coordinate its attack on Georgia during a five-day war in 2008, taking out key news and government websites as tanks rolled into those specific cities.

As a result, law enforcement tolerance for hacking has fallen to zero. In 1999, the hacker Space Rogue exposed how FAO Schwarz's website was leaking consumer email addresses and forced the company to fix it. He was cheered. When Andrew Auernheimer (known as "weev") did the same thing to AT&T in 2010, he spent more than a year in prison until his case was overturned on a technicality.

The days of mere curiosity are over.