Orange Podcast – On the line – Nicolas Arpagian

Orange presents On the line.

Journalist: Today we'll be spending 5 minutes face to face with Nicolas Arpagian. You're the Director of Strategy and Public Affairs at Orange Cyberdefense. Hello Nicolas.

Nicolas Arpagian: Hello.

Journalist: So first of all, what does your job involve?

Nicolas Arpagian: Our job, is to make using technology, which is now everywhere in our everyday personal and professional lives, as safe as possible. To ensure that the data we produce, the data we store and value, and also the browsing we do online or on our various devices (phone, smartphone, tablet or computer) is as protected as possible to avoid losing data or not being able to use the devices themselves because they no longer work.

Journalist: Safeguard against a hacker, that's what it means?

Nicolas Arpagian: Against a hacker, because indeed there are risks if we don't take certain precautions, it can weaken our digital safety, our online activity, you have to know the nature of the threats, the main threats in order to protect yourself.

Journalist: So concretely, for example, put it into context: give us three situations that we must avoid, 3 tips?

Nicolas Arpagian: The first thing already: install an antivirus. That's to say protect against known malware, that's the first thing.

Journalist: It's basic.

Nicolas Arpagian: It's necessary, yes, but it is also necessary to keep it up to date. Secondly: update your browser. Whatever you use: Firefox or Internet Explorer, Chrome, whatever you're using to surf online, you have to update it. Why? Because with each update you'll benefit from all the knowledge concerning all the malware that has been identified and the update helps to protect against it all.

Journalist: But I can always do it another day…

Nicolas Arpagian: So that's unfortunate because actually you could be benefitting right now from these latest updates. Because when malware is identified, it's necessary to avoid the hacker who also knows about it and can use it against you because he knows you haven't carried out the update.

Journalist: OK, I'll update everything as soon as I'm prompted from now on. Another thing to be aware of?

Nicolas Arpagian: The third thing you have to do is make sure you make copies, back up your data on a hard drive, even on a server if possible (we talk about cloud where data is stored on servers) because if at a certain point your computer is hacked you can limit the impact of the attack because you have a way to recover most of your data. So even if you've failed to prevent the attack, you can reduce the impact of it and be able to return to normal as soon as possible.

Journalist: At work, can I still have a private life, be left in peace to check Facebook?

Nicolas Arpagian: So you can have a private life, but not a digital private life.

Journalist: How so?

Nicolas Arpagian: Why? Because Facebook, for example, as you say, is very revealing about your interests, when you like something or other.

Journalist: And so?

Nicolas Arpagian: And so the problem is that hackers can easily find out the things you're into, which means everything you click on, everything you download, and at that moment they can send you infected data. It's not really your Facebook account that would be affected, but your work computer, which means someone could access your email, the company server and therefore even accounts or research and development. In short, you are at that moment a point of weakness because under the pretext of clicking on something, which you can't verify in terms of its origin or integrity, you're opening the door to your corporate data and therefore making it vulnerable.

Journalist: Can this hacker hack something other than my computer?

Nicolas Arpagian: So in fact any information that allows access to a service. Think for example of the access badge you're given to enter the office. In fact it's a pass. A soon as you leave it on a table in a café, in the canteen, you only need to leave it for a few seconds in fact and someone can scan it and create a clone, its twin, which means it can also let someone enter the building in your place and have all the same access given to you by your employer.

Journalist: It's scary!

Nicolas Arpagian: But it has to be thought about because it's not science fiction! The hacker, every time, will find a way that lets him carry on in peace. In fact, rather than creating false identities, he'll just try to mimic what you do so he can move around comfortably in your shoes without attracting attention, capture information and enjoy all your access rights as a legitimate user.

Journalist: So if I, for example, if I bring a USB key to work, which is infected, if I put it in a networked computer, the virus can spread throughout the network?

Nicolas Arpagian: So, since you cannot assume whether it's infected or not, you're right to think that you shouldn't use a USB key in the workplace. Why? Because you're not sure of the integrity of this USB key. You might think that because you can see all the files on it, you have a complete view of everything that's on it.

Journalist: And that's not the case?

Nicolas Arpagian: Of course not, because the hacker is careful, when he puts malware on it, the programme won't appear on the menu and therefore it's true that the USB key you find in the parking lot or pick up at a tradeshow may well contain a hacking tool. So, avoid using them even if they're handy, because it's a very accessible and effective gateway for malicious hackers.

Journalist: Nicolas Arpagian, you're the Director of Strategy & Public Affairs at Orange Cyberdefense and we've heard what you've said. I'll update everything as soon as I'm prompted, I'll stop leaving my badge on the bar, I will keep my personal USB key at home and I'll stop going on Facebook. Thank you so much.

Nicolas Arpagian: Thank you

This was On the line, an Orange podcast.