Episode 4

A shadow industry of fraud

MONSTER under the BED

Podcast: Monster Under the Bed

For further information on the EIB's activities, please consult our website, www.eib.org. You can also contact our info Desk, info@eib.org.

Published by the European Investment Bank.

A shadow industry of fraud

Monster Under the Bed

Transcript: Episode 4

Intro

Allar: Don't be scared. This is the podcast that always leaves the light on.

Music

Allar (over the music): This is Monster Under the Bed. The podcast that takes some of the fears and myths in our society and busts them wide open. I'm Allar Tankler.

End of intro

Thomas: Well, once I was just playing a game called Fortnight with my cousin and then suddenly it just said you couldn't play anymore, a screen popped up. I was trying to go back into the game but I couldn't.

Chris: How did you feel about that?

Thomas: At first I thought it was a glitch and then my dad told me it was a hacker, and I was kind of stressed because I was scared he would steal and do a lot of stuff to my account.

Allar: Chris, who's that kid?

Chris: That was my kid, Thomas. He's 10. He plays some games online and his account was hacked about a year ago. He's still worried about it today.

Allar: What did the hackers do, Chris?

Chris: Well, fortunately they didn't do much. They changed his user name. They changed his logo to some scary image. But we did get the account back and we added a better password.

Allar: Are you worried about your kids using computers?

Chris: I do want them to explore the Internet and open their minds, but I do worry that they'll click something that lets a hacker clean out my bank account.

Allar: I have to admit, I don't think about cybercrime that often at home or at the office.

Chris: There's a myth that if we have the latest software on our computers, and we have a strong IT department at work, then we are safe from cyberattacks.

Allar: So the issue is: We all think we're safe. But we're not?

Chris: Remember in the first episode of this series, Allar, you talked about leaving a light on because of the monster under the bed?

Allar: Of course. The monster under the bed, which doesn't exist.

Chris: Well, in this case, there IS a monster under the bed, but few of us bother to leave a light on… And that monster is cybercrime.

Allar: And this myth that we're safe is causing us to lose money? Are you going to tell us how to turn on the light?

Chris: Yes. You definitely should not simply rely on software updates or the IT department to protect you.

Allar: So today on Monster Under the Bed…

Chris: Keep safe from cybercrime…Think like a hacker.

Allar: Monster Under the Bed is a podcast from the European Investment Bank, the EU bank. We're exploring different fears and beliefs people have which are costing us as a society. In each episode of the podcast, we fight one imaginary – or, in this case, an underrated monster under the bed and win the battle for a more rational way of doing things in the spheres of education, healthcare, climate, and many others.

Chris: I'm Chris, and I work with Allar at the European Investment Bank. So that you don't miss an episode, subscribe to Monster Under the Bed on iTunes, Acast, Stitcher, player.fm or wherever you get your podcasts.

Allar: And let us know if you can think of a monster we should expose on future episodes. Get in touch with me on Twitter @AllarTankler or you can just tag @eib.

Allar: So Chris, you said we should think like a hacker? What does that mean?

Chris: Good question. I talked to several cyber security experts. They told me we need to think more about how we might be hurt by cybercrime and what we can do to prevent attacks.

Jonathan Lusthaus: I mean I think the point about the IT department is important because in a way that is a crutch people use. They think they can rely on others to keep them safe. The sad reality is you can't. Obviously having

a good IT department is really useful, but there's a huge amount of this that really comes down to individual users.

Chris: That was **Jonathan Lusthaus**. He's a sociologist at the University of Oxford and an expert on cybercrime. He spent seven years talking to cyber criminals for a recent book. Jonathan told me many ways to fight cybercrime, but he said it comes down to changing the way we think and act.

Jonathan: So if we think about many attacks that are happening, there's often a human element to it. So we might think of these things as being very technical, whether it's involving malware or something else, but often for that malware to be engaged, for it to actually play the function that it's designed to do, this requires someone to click on a link or attachment or to visit a suspicious website or whatever that might be. And so what that means is that even in these very technical types of attacks we're often seeing that human element. Which means that each person has a responsibility for keeping themselves safe but also keeping the organisation safe.

Allar: I wonder how the IT departments feel when someone calls them a crutch?

Chris: I wondered about that, too. I asked IT experts at the European Investment Bank, and they agreed with Jonathan, believe it or not. They said there is only so much they can do. Here are **Vicky Politopoulou** and **Jacoba Sieders** explaining why they can't protect us all the time:

Vicky: An IT department is just a security control. So all security controls can fail at some point, but we should change our attitude. We should be aware of the risks that we have. So we cannot just relax that a good IT department can protect us.

Jacoba: For instance, there are so-called zero-day attacks. That's a new attack that our IT department doesn't know about. A big vector way to attack would be sending emails, phishing, make you click on a link, click an attachment, and there could be nasty stuff in that. And things start executing on the network. And if that's a new type of attack, no one knows how to work with it. And they could steal money or encrypt the whole entire content and ruin a lot of businesses. And that's all the time happening, every day new zero-day attacks are coming.

Vicky: A good IT department can make things harder for an attacker. The attackers are one step ahead and we are just trying to catch them. So it's a game of cat and mouse.

Jacoba: Constant rat race.

Allar: So we need a new way of thinking. How important is it that we address this problem? What if we just do nothing?

Chris. Hacking will keep getting worse, and part of the reason is the profit. One recent study suggested that cybercriminals are generating more than $1 trillion a year in revenue and this isn't going to slow down, because cybercriminals are getting more sophisticated and working more often in groups. Cyberattacks are causing big losses to the global economy and not all of these attacks are reported, because some companies are embarrassed or scared to reveal them.

Allar: The European Commission says there are several thousand cybercrime attacks a day in Europe and that most European companies have experienced a cybersecurity incident.

Chris: The cost of cybercrime has doubled in the past few years. The World Economic Forum has named cybercrime one of the planet's most critical issues, in addition to climate change and Christmas coming to the shops earlier every year. The European Investment Bank, the EU bank, has made investing in cybersecurity a priority, partly because preventing hacking helps keep companies' balance sheets healthy and it's good for the economy. I asked **Anders Bohlin**, a digital specialist at the Bank, if it's enough simply to update our computers and hope the IT department can do the rest.

Anders: One could make the comparison, do you trust the red light at a crossing? One has to be aware that it's down to individual behaviour. The IT department is a very important toolbox for a company to make sure that we have the sort of technical tools in place, but if one individual in an organisation is not following the procedures, you're opening up a back door into the company.

Allar: So what can the European Investment Bank do about this problem? We're not a software firm.

Chris: You're right, we're not a software company. The people at the Bank working in technology investment tell me that companies are surprised when

they hear that we can do a lot to help them fight cybercrime. There are several areas where the Bank can get involved: We invest in companies developing advanced software that protects people's data, we're helping companies hire more computer experts, and we remind companies that when they're making investments in new technology, they should invest in cybersecurity to keep this technology safe.

Allar: This is a huge, global problem. Just who are these hackers?

Chris: The hackers could be your neighbour or colleague. The hacker could be a mile away or a continent away. Here's Jonathan Lusthaus again, describing the average cybercriminal.

Jonathan: Overall, the young hacker stereotype is a little outdated now. We're still seeing people like this, involving younger offenders messing around, maybe not understanding what they're involved in, but we've reached the point now that we're really looking at something highly professional and highly organised. And so when they're starting to get into that part of this work, it really starts to become much more like a business, like a job for them. And there are certainly former offenders I've spoken to where this was their job, this was earning them a substantial amount of money, this is what they did. While I also spoke to others where it was not their only job, but it was a core job, a second job or they're running multiple business, some of them legitimate and some less than legitimate. But in a lot of these cases there was a large amount of money being made, and that was kind of a key driver in terms of why they were involved. The final point -- could it be a neighbour or co-worker? It can always be, you never really know who's who when talking about these sorts of things happening online. But the point about that really is one of the threats people ignore. They're always looking for an external threat, someone outside of an organisation. But one of the things we see is insiders are also quite a big threat. So when we talk about, "Could it be my co-worker?", that's exactly the type of threat we're talking about. Someone within an organisation who might be turning against that organisation for a number of reasons and those people can be extremely damaging if they make that choice.

Allar: So hackers are everywhere. That is scary. Perhaps now it's time to give listeners some advice on staying safe. Are there dos and don'ts we can list?

Chris: Three experts at the Bank, Vicky, Jacoba and Federico Paroline, told me their favourite tips for adults and children.

Vicky: First of all, we all should use strong passwords. And we should not use the same passwords for everything, so please don't use the password that you have for your bank account or your website or your online banking website with the password that you have for Facebook.

Jacoba: We did research in the Netherlands across all the banking people, four banks together, 4000 people, and we found the privacy paradox and the password paradox. Most people know they should use a difficult password, they should refresh it, they should not use it in various environments, the same password, but still they do, even I do. I'm a security person. That's what we call the privacy paradox. People are worried for their data and their security and at the same time they're at ease, so security and ease of use are always fighting each other. So always choose security and not ease. That's the message

Federico: Another important part is also that you have to keep your software up to date, not only here at the bank, because the IT department is taking care of that, but also at home. With your personal laptop, you should always maintain your software up to date. Also get an antivirus, because for example we had a ransomware attack. You receive an email and you click on a specific link and the computer starts to be encrypted completely, so you lose access to all your data. So imagine that you can't access your document anymore, your image anymore. You click on it and you get just a window saying you have to pay to get your data back. We are not just talking about our personal life or your personal laptop, because we had in Baltimore in the U.S., all the computers of the city were attacked by ransomware and they were with Windows XP. So we're talking about an old legacy software, not supported anymore. They didn't upgrade all the computers and they were attacked with ransomware, and that was really a big problem.

Vicky: We should not download from untrusted sources as well, because we have seen many instances that someone downloaded an update of the software from a source that had malware. So update the software from trusted sources as well. This is something very important.

Jacoba: The biggest and easiest is to never click that link, never open untrusted email, be very aware of that. With ransomware, then you have to pay a ransom to get your data free. If you make your backup, you don't need to pay, because you have your backup. So I make backups of my private data every week. So for that part, I'm safe, even if I click some link.

Vicky: Something else: We should not reveal too much information on social media. Children as well. So we have to teach our children that they should not reveal information if they are on holidays, for example. Because a thief may read these posts on Facebook and they could come and be at our home to steal valuable things from us. So publish as less as you can. This is our advice.

Chris: Jonathan Lusthaus told me that the simplest solutions help the most, but many people don't even do the minimum.

Jonathan: There are obviously some simple ideas that really most people should be doing, so you've mentioned a couple -- having strong and diverse passwords, having basic software in place, whether it's an antivirus, having a firewall activated on your computer. These sorts of things are quite simple to do, but not everyone does them. But that brings us to a broader point, which is, even though some of these things could probably be quite easily done by a lot of people, they're still not being done, and this is even after people are being encouraged to do them. And so I think in some sense this situation is more complicated for the average user, even than those in the tech sector would like to think. For me, really, if we're going to have one message, it should be a message of being cautious. If that's one thing people can take out of the cybersecurity discussion, it's to be aware of the dangers out there, be aware that there is this kind of shadow industry that is really spending time trying to figure out how to defraud people and attack them in various ways.

Chris: The experts had others tips, too. People and companies need to report cybercrime more often, and countries need to cooperate more across borders to track down cybercriminals. Banks need to share more data about the origins and the amount of attacks. Here are Jacoba and Federico once more, talking about the importance of working together and reporting crimes:

Jacoba: I'm from Holland and there the banks are connecting and sharing the bad guys' data with each other and I think if that happens across every domain, not just tech companies, the banks but also the governments and police, I think that would be the only way to stop it. But we need everyone to help us. And I would say to everyone, "Think like a hacker." Never click links, never open attachments. If everyone did that, I think we could contain a lot of damage.

Federico: If you see something, please report it. You have to report if there is a data breach. If you see something that is strange, it could be strange, you have to report it. This is the only way to fight cybercriminals.

Allar: Well, you have almost scared me off using a computer. So what about the future?

Chris: Well, I should tell you, the near future doesn't look good. We do hope to slow down cybercrime, but the hackers will get even more sophisticated and crafty.

Federico: The hackers are smarter every day.

Jacoba: They work like a corporate. I think it will keep growing. It will be endless.

Vicky: We like challenges.

Federico: Unfortunately, the bad guys, the hackers, they're always ahead, so we can, with the firewalls and everything, catch the majority of hackers, but the ones in the lead will always be in the lead.

Allar: Well, thanks for giving us the most worrying podcast so far.

Chris: Cheer up, Allar. My kids have a simple suggestion and I love it.

Allar: Will it make me feel better or worse?

Chris: See what you think.

Thomas: I would say, "Stop doing it."

Juliette: Yeah, stop doing it, because it's rude.

Thomas: Be a normal person, not a hacker.

Juliette: Play with somebody else and not hack somebody!

Outro music

MONSTER under the BED

European Investment Bank
The EU bank