Down to Business English

114 - The WannaCry Ransomware

Record Date: May 28, 2017

www.downtobusinessenglish.com

From Tokyo Japan and Auckland New Zealand, this is Down to Business English, with your hosts Skip Montreux and Samantha Vega.

Samantha: Finally we make it back behind the microphones again, Skip.

Skip: Yes. Our schedules and the time difference between Japan and New Zealand certainly have not been cooperating recently, have they?

Samantha: No, they haven't.

Skip: So, Samantha, how are you? Doing well?

Samantha: Yeah, yeah, pretty much everything is fine, but ...

Skip: That sounds like a pretty serious 'but' there.

Samantha: It is, everything is fine, but - and this has just been happening over the last couple of days - my laptop **is on its last legs**, so it's really kind of painful to get anything done. It's kind of a first-world problem, but I really need to replace it soon.

Skip: Are you backing up all your data?

Samantha: Well, pretty much, yeah. You know, I'm pretty good at keeping important files backed up. On the cloud now – used to be a terabyte, and then you'd have to get a terabyte to back up your terabyte and that sort of thing. But if my hard drive ever crashes and I lost all my data, I'd just want to cry.

Skip: Well, that's funny you would just want to cry.

Samantha: Uh, why is that funny?

Skip: Well, today's topic is about the WannaCry cyber attack that took place earlier in May.

Samantha: Oh yeah, that ransomware attack. That's what it was called, "I want to cry" ?

Skip: Actually, it was just called the Wannacry ransomware.

Samantha: Well, very aptly named I guess. It sure made headlines when it first kinda hit, but then it kind of fizzled out.

Skip: It may have fizzled out from the media's attention, but the implications of this attack are quite significant for business. So I thought we should explore this topic today.

Samantha: Okay, sounds good.

Skip: Great, so let's do it. Let's get D2B with the WannaCry ransomware attack. What is it, how did it affect businesses around the world, and what you should do if you or your organization is infected.

Samantha: Well, maybe the best place to start is to bring everyone up to speed on what ransomware is.

Skip: Sure, are you very familiar with it?

Samantha: Well, thankfully, I've never been affected by it. But yes, basically I understand the concept. A hacker breaks into your computer and covertly installs software that locks all your files. The only way the user can get back access to their files is by paying a ransom to the hacker.

Skip: Yes, that is the basic concept. And this type of **extortion** has been around almost since the beginning of the internet.

Samantha: Really? Since the early eighties?

Skip: Actually more like the late eighties. The first known case of ransomware was in 1989. It was called the AIDS Trojan Malware.

Samantha: No, I never heard of that particular one, but there've been many different kinds of attacks over the years.

Skip: True. Cyber security is a big part of any IT department's workload, and over the

years, the general population has become more aware of the dangers of computer viruses.

Samantha: That's why I never click on a link in an email I receive from a stranger. The potential of getting your computer hacked is just too great. What are the specifics of this WannaCry attack? What makes it so different from previous attacks?

Skip: That is a good question. The issue with the WannaCry attack was how widespread it was and how quickly it spread around the world. It was released on Friday, May 12th, and within three or four days had spread to over 150 different countries and infected over 200,000 computers.

Samantha: That's a lot of people clicking on malicious links. I thought people would have known better by now.

Skip: Well, it wasn't just a matter of clicking on malicious links. The virus was designed to infect all computers connected to the same system. So if your coworker, for example, clicked on a link and got infected, then every computer, including yours, on the entire system would be infected. It was a very contagious virus.

Samantha: Ah, that's why we got all of the emails from IT over that, as soon as it was released saying, "Don't open up any strange files." And what was the ransom, anyway? What did the perpetrators want in order to unlock the files?

Skip: The hackers demanded $300 USD paid in bitcoin, and that ransom doubled every three days.

Samantha: And uh, oh... and also, I guess since the attack was on a Friday, most users didn't know about it until they went to work on Monday and the ransom had already doubled.

Skip: That is exactly what happened.

Samantha: Wow, talk about having a terrible start to the week. Coming in on Monday morning and not being able to access any work files. The hackers must have made a mint.

Skip: Actually, one very interesting **takeaway** from all of this is how little money the hackers actually made.

Samantha: That's surprising.

Skip: Very surprising. Even though it's the most widespread ransomware attack in history, and even though it targeted a huge number of companies like FedEx, Nissan, Telefonica in Spain, the National Health Services in the UK. In Russia, the central bank and the interior ministry were attacked. Even some of their railway systems were hacked. But even though all of these big victims could quite easily pay the ransom, so far, less than $100,000 USD has been paid.

Samantha: Sounds like a big bust for the hackers then. I noticed in that list that there are very few US companies in the mix. The UK, Spain, Russia, but not so much the US.

Skip: Well, FedEx was affected, but they are more international than some of the other victims.

Samantha: So why was that?

Skip: Well, that's another interesting **takeaway**. The WannaCry virus was based on an **exploit** in older versions of Microsoft operating systems.

Samantha: Microsoft must have **been in the hot seat** for that.

Skip: Actually, no. Microsoft knew about this security hole and had released patches to rectify the **exploit.** The problem is that many organizations outside the US failed to install the security patch.

Samantha: Why would they not do that?

Skip: Well, mainly it is costly and labor-intensive to keep huge systems up-to-date. Take for example the NHS in the UK. They have thousands and thousands of computers. They were doing their best to protect themselves from viruses, but the IT department just didn't have the budget or the resources to keep up.

Samantha: I suppose when a business is dealing with thousands of computers in their network, the decision to update to the latest operating system is a substantial one.

Skip: Well, what we learned from this attack is that it mainly infected companies and organizations using Windows 7 and even XP.

Samantha: XP? People still use XP?

Skip: More than you think apparently. And I think this is one place, I think, that Microsoft really went out of their way to help the public. XP reached its EOL three years ago in 2014.

Samantha: Sorry, what's EOL?

Skip: EOL stands for End Of Life. Since April of 2014, Microsoft hasn't been supporting XP with bug fixes or security updates.

Samantha: That's right, I remember that. I used to use XP. I used XP for years, actually. I really liked it as an OS, but I stopped doing it, I stopped using it, just because of that.

Skip: Well, having said all of that, when the WannaCry virus did show up in the wild, Microsoft released a fix for XP users. A very unusual step, as they were under no obligation to do so.

Samantha: Okay, so how was the attack stopped?

Skip: Very interesting story behind that. Fortunately, a very sharp security researcher by the name of Marcus Hutchins studied a sample of the WannaCry virus's code. What he noticed was there was a URL in the code, and he also noticed that that particular URL wasn't real. In other words, it did not exist on the internet. Now, not knowing exactly what it was for, he gambled and spent $10 and registered it and made it an active website. It turns out that once it was active, it acted as a kill switch for the virus, effectively stopping the spread.

Samantha: Wow, so he did it **by fluke**.

Skip: Yes. Very scary, but true.

Samantha: Wow. Something tells me even though the hackers didn't make much money this time, that this WannaCry virus is just the beginning of more ransomware.

Skip: I agree.

Samantha: Yeah, look what happened to Disney just last month.

Skip: Right.

Samantha: Yeah, hackers got their hands on a copy of the final version of Pirates of the Caribbean, and demanded an undisclosed ransom, or else they'd start releasing the movie on the internet.

Skip: But Disney refused to pay, and the pirates never actually released the movie. In fact, I've heard that it could have been a hoax.

Samantha: True, it could have been a hoax, but one case that wasn't a hoax was what happened to Netflix. Did you hear about that? Hackers did release the first half of season five of Orange is the New Black, one of Netflix's most popular titles, after they refused to pay ransom demands.

Skip: Yes, but it remains to be seen if that will translate into a loss for Netflix. I don't think users will close their account just because one of the Netflix titles is available for free online.

Samantha: True. Their business model isn't dependent on just one program after all, is it?

Skip: In any case, cyber crime, **extortion** on the internet, and ransomware will certainly continue to be an issue as we go forward.

Samantha: I'm sure it will. Everyone just needs to keep their data backed up, secure, and remain vigilant when clicking on suspicious links.

Skip: That is good advice. But, Samantha, why don't we now get D2V ... Down to Vocabulary.

Down to Business English audio scripts are a great learning tool. Be sure to visit the D2B website and download your free audio script to today's podcast. downtobusinessenglish.com. That's www.downtobusinessenglish.com

Skip: Memberships….memberships...get your D2B memberships here!!

Samantha: What are you doing?

Skip: I'm advertising.

Samantha: Advertising?

Skip: What does it sound like?

Samantha: It sounds like you are one of those shady street touts on Koh Samui, selling cheap hotels to tourists getting off the boat.

Skip: Really? That wasn't the brand image I was going for. I just wanted to encourage all of our listeners to support the show by becoming a D2B member.

Samantha: Well why don't you just explain who the memberships are for? That might be more attractive to everyone listening.

Skip: Okay, let me try again. Can you set it up for me?

Samantha: Okay sure. So Skip, who are D2B memberships for?

Skip: That is an excellent question Samantha. Let me explain. If you value Down to Business English, if you enjoy our shows and would like us to release episodes more regularly. If you would like access to our COMPLETE library of audio scripts without having to fill in an annoying online form for each individual episode. And if you would like the benefit of having audio scripts of new episodes emailed directly to you ... then you should be a D2B member.

Samantha: I see. And exactly how much does a membership cost?

Skip: Another excellent question. We have four membership plans to choose from. A monthly membership for $7.00 a month, a 3 month quarterly membership for $19.50, a 6 month semi-annual membership for $36.00, and a 12 month annual membership for the low price of $66.00.

Samantha: Well, that is a pretty good deal. 66 bucks for 114 audio scripts …

Skip: 114 and growing!

Samantha: And growing, yes. And the great thing is, the more listeners who become members, the faster that number will grow.

Skip: Exactly! So everyone, help us help you with your business English. Visit our website, downtobusinessenglish.com, click on the **Membership link** at the top of the page, and become a D2B member today!!

Samantha: There, that sounded much better than a street tout.

Skip: I agree. Shall we get on with the vocabulary.

Samantha: Yes, let me start things off with the an idiom I used in the opening of today's episode. – to **be on your last legs**. When you say something **is on its last legs**, you are saying that it is near the end its useful life. When Skip and I were talking about my laptop, I mentioned that it **was on its last legs**. In other words, it is not running very well and is probably going to stop working very soon.

Skip: You can also use this idiom to communicate that you are really tired. For example, if your boss invites you out for Friday night drinks at the end of a long week, and you want to politely decline the invitation, you can say something like, "Thanks, I'd really like to but I've worked overtime every night this week and **I am on my last legs**. I think I should just go home and get some rest."

Samantha: Skip, it sounds like you have used that excuse before.

Skip: I have. But I hope you are not calling me a liar.

Samantha: Of course not. What is our next word?

Skip: Next up I want to talk about the noun **extortion**. From a legal point of view, **extortion** is when one person forces another person to pay some money by threatening them with some kind of harmful act.

Samantha: In the story you said that **extortion**, in the form of ransomware, has been used on the internet for a long time.

Skip: That's right. In other words, since the beginning of the internet, criminals have used ransomware to force people to pay money in order to regain access to their data.

Samantha: **Extortion** doesn't always refer to a criminal activity though does it?

Skip: No it doesn't. You can use it in a non-criminal way as well to indicate that you feel you are being overcharged or treated unfairly. For example I recently tried to change the mobile phone carrier I use. But when I called my current carrier to cancel the account, they informed me that there was a ¥10,000 yen cancellation fee.

Samantha: ¥10,000, just to cancel your account?

Skip: Absolute **extortion** if you ask me.

Samantha: It does seem quite unreasonable, yes. The verb form of **extortion**, to extort, is also commonly used isn't it?

Skip: Yes it is. The other day, I was reading a news story out of Bangladesh about how a small group of police are actually **extorting** travelers as they are traveling to their hometowns during the Eid festival.

Samantha: The police **extorting** travelers? How does that work?

Skip: Apparently a group of bad cops are stopping busses on the highway and threatening to take the passengers' belongings unless they pay an additional fee for using the road.

Samantha: A classic example of **extortion.** I guess the **takeaway** from that is it is hard to trust anyone these days.

Skip: **Takeaway?**

Samantha: Yes, **takeaway,** which is our next word.

Skip: And what is a **takeaway**?

Samantha: A **takeaway** is the main point you learn from an experience or event. In the story, Skip commented that one interesting **takeaway** from the ransomware story, is that the **extortionists** did not make very much money.

Skip: In other words, a key point to the story is that victims of the attack chose not to pay off the criminals.

Samantha: A very wise decision if you ask me.

Skip: Can you give us another example using **takeaway?**

Samantha: I sure can. Did you follow the results of the recent UK election?

Skip: Yes, I most certainly did. The Conservative party under Prime Minister Theresa May sure took a beating.

Samantha: Well, one **takeaway** from that is upcoming Brexit negotiations between the EU and UK just became even more complicated. With only a minority government, May is not going to have the political power to negotiate from a position of strength.

Skip: Nice example. Next up today is the idiom to **be in the hot seat**. I think the meaning of this phrase is easy enough to imagine – when you **are in the hot seat**, you are in a position where people are holding you responsible for a problem, and you have to answer for what caused that issue, and perhaps offer a solution. In the story, Samantha thought that since the ransomware mainly attacked Windows operating systems, that Microsoft **was in the hot seat**. In other words, many people were holding Microsoft responsible for allowing that problem to happen.

Samantha: Have you ever **been in the hot seat** Skip?

Skip: Oh most definitely. I have several business English teachers working under me and when there is a problem in their course, my boss looks at me for answers. Fortunately, I have a very good team and it doesn't happen that often. And you? Have you ever **been in the hot seat?**

Samantha: I'm sure I have, but nothing too serious. But let's move on.

Skip: Good idea, what is our next word?

Samantha: Our next word is the noun **exploit** which can be used in two different ways. The first meaning of **exploit** is an exciting adventure or experience.

Skip: Like back in the days when you lived in Tokyo. Our circle of friends sure had a lot of fun **exploits** on the weekends. I have a lot of good memories of those parties we went to.

Samantha: Ah yes, Tokyo was a blast. But getting back to **exploit,** the second meaning, and this is the way we used it in today's story, is a piece of software that takes advantage of a weak point in a computer program. In the story, Skip reported that when Microsoft found out about an **exploit** in their operating systems, they released security patches to fix it.

Skip: In other words, Microsoft discovered a weak point in their computer code that made it possible for hackers to attack a user's computer.

Samantha: Precisely.

Skip: In a business context, **exploit** is often used as a verb. For example, the whole purpose of market research is to gather consumer information so that a company can learn how to **exploit** potential customers.

Samantha: I don't know, that sounds a little negative to me. Market research is about learning what the customer wants, not about **exploiting** them.

Skip: True, the word **exploit** does have a negative nuance. But as I am a bit of a cynical consumer, I view all market research as **exploitive**.

Samantha: You need to relax. What's our next word?

Skip: Our next, and final word today is the expression, to do something **by fluke**. When you say that you did something, or something was done **by fluke**, you are saying that it was accomplished through luck or by chance, not through skill.

Samantha: In the story, after hearing about how Marcus Hutchins stopped the WannaCry ransomware attack, I commented that it was **by fluke**.

Skip: And it was. He stopped the cyber attack by chance. He just had a lucky idea, tried it, and it worked.

Samantha: Well, **fluke** or not it is a good thing he was able to stop it. Can you give us another example of doing something **by fluke?**

Skip: Yesterday I was watching videos of past World Series of Poker events on You Tube.

Samantha: You are watching people play cards? Isn't that a little boring?

Skip: Not to me. Now, these tournaments are open to everyone, all a person needs is to pay the $10,000 entrance fee and you are in. The result is that you often see professional poker players competing at tables with amateurs.

Samantha: Kind of like Pro-Am golf tourneys.

Skip: I suppose so. Now, one **takeaway** I get from watching these poker videos is that you can really see the skill difference between a pro and an amateur.

Samantha: How much skill can there be in poker? It's just luck isn't it?

Skip: Oh dear no. Luck is just a small part of the game. It takes a lot of skill to **exploit** the maximum number of chips from your opponents when you do get lucky cards.

Samantha: If you say so.

Skip: I do. For the most part, pro players end up winning tournaments, but there are times when an amateur wins. When this happens, it is usually more due to **fluke** than overall skill.

Samantha: Are you saying amateurs shouldn't be playing in the World Series of Poker?

Skip: Oh no not at all. I think it is a great system having pros and amateurs play together. In fact, I dream of playing in World Series Of Poker and **fluking** off a win.

Would you like to support Down to Business English? Be sure to visit the D2B page in iTunes and subscribe to the show. While you are there, why don't you leave a rating and a comment. This will help D2B reach more people wanting to improve their Business English skills. Down to Business English. Business News, to improve your Business English.

Samantha: Well thanks for that report on the WannaCry ransomware story Skip. I hope none of our listeners were affected and that everyone is regularly backing up their important data and files.

Skip: Great advice. Even though this attack ended up being relatively harmless on a global scale, there are sure to be similar attacks in the future, so I have three words for everyone.

Samantha: And what are they?

Skip: Backup, backup, and backup.

Samantha: Yes, very important.

Skip: Just on a side note Samantha. Do you know the 3-2-1 rule of back up?

Samantha:: No, I don't think I do.

Skip: To really consider yourself backed up you should have 3 backups, on 2 different kinds of media, and at least one of them should be stored offsite.

Samantha: Really. Well in that case I guess I'm not as 'backed-up' as I should be.

Skip: Well, you had better take care of that as soon as you can.

Samantha: I will be sure to do that. Thanks for listening everyone. See you next time.

Skip: Take care.

Have a comment or question about today's show? Don't be shy. Visit the D2B website or the Facebook page, and post any comments or questions there. Skip, Dez, or Samantha will be sure to leave a reply.

Want to get even more Down to Business English? Sign up for the D2B newsletter and receive updates on some of the stories covered on Down to Business English. That's www.downtobusinessenglish.com.

Down to Business English... Business News, to improve your Business English.

Useful Links

For easy access to online Dictionary definitions, use these links:

- *to on one's last leg (idiom)*
- *extortion (noun)*
- *a takeaway (noun)*
- *to be in the hotseat (idiom)*
- *an exploit (noun)*
- *to exploit (verb)*
- *a fluke*

Learn more about how computer viruses spread

- *5 of the Worst Computer Viruses Ever (You Tube)*

Read more about how to protect yourself from the WannaCry computer virus

- *How to protect yourself from WannaCry ransomware*