Centre of Excellence
DIGITAL INNOVATION

The First Cyberattack?

Title of Activity:	The First Cyberattack… in 1837?
Overview:	Below is the AI generated transcript from the podcast episode: 1E5: Human Insecurity from Slate Magazine's "Slate Technology Feed" podcast series. Note: The transcript was generated by running the audio file from the podcast through Microsoft Office's AI-powered transcription service. There may be inaccuracies and grammatical mistakes.
Additional Information	For additional activities, information, or how to contact us, visit our website: https://centresofexcellencenb.ca

Hello Jennie standige.

Hello Mommy, it's Tom here how are you?

I'm OK thanks yes.

This is my mum. She emailed me the other day to say she'd been hacked.

Well, I was rung up by somebody and he said he was a BT Internet man and he said he was going to shut our Internet down. In order to help me to stop other people interfering.

During last week, she'd been rung up by someone who said they were from her broadband provider.

Got me onto the computer and got me to open stuff.

They managed to persuade her to turn off her firewall and install software on her computer that they could then use to take over her computer.

They wanted to get into the router and they wanted to put security in the router for the NatWest account. And for my Sainsbury's bank account.

They got her to log into her online bank accounts and they spun her some yarn about doing security checks, which was really all just a trick to get her to give them the codes that they needed to start moving money out.

Of her account, and at that stage they were sort of like fiddling around.

Thank you.

They've got control of my mouse that they've got in and they've.

Right?

Got control and I like couldn't stop it. I should have stopped it much. Earlier than that. And that is so plausible. I can't believe I was so hoodwinked. I really can't. They told me they were trying to fix it so it's secure.

And then of course, the bank rang her up and said someone was trying to move 9000 pounds to India. And did she really mean to do this? And she's ended up having to close one account and disable online banking on the other? And I had to go round like that evening and clean all the crap off. Computer before she could use it again.

But what would have happened if I had finished the call when he was inside the box? And everything please help me.

He wasn't really inside the box, so I think they made you go and look at the router in the other room so that you wouldn't notice what was going on. The screen of your computer which was they were setting themselves up as a as a payee anyway, don't beat yourself up about it. It happens to lots of people, and it's the main thing is that you know the bank stepped in and and nothing bad has happened and it won't happen again.

Right?

Don't thank you very much for reassuring me.

Come on, you might let it happen again.

It certainly won't excellent.

OK, well great talk to you.

Yeah OK, thanks very much, yeah.

See you soon bye. I mean, I suppose it's a sign of the times because it used to be the only network managers and. You know it gurus. Had to worry about people trying to break into their computers and do bad stuff and now it's a problem that affects everyone, even my mum.

It feels like it's getting. Worse, no matter how much technology we apply to the. Problem so. We've got firewalls. Antivirus software passwords and two factor authentication and fingerprint readers. People are spending millions of dollars defending against these hacks, but the hacks still keep happening.

And the consequences are getting more serious. There are these big attacks where millions of people have their personal information stolen, like the Equifax hack. And then there are the ransomware attacks, which is where a virus gets onto your computer and encrypts all your data and then demands money. And unless you pay the money, it's all scrambled and you can't use it anymore and in 2017. Several hospitals and car factories and even ports around the world had to actually shut down because their systems were infected by an example of this kind of ransomware. And it's not just cybercriminals trying to make a quick buck. This has taken on geopolitical dimensions. We've also had Stuxnet, for example. A virus probably designed by Israel, which was intended to sabotage the Iranian nuclear program. And we've got Chinese state hackers breaking into Western companies to steal blueprints and other valuable intellectual property.

Hacking can be hard to understand at a technical level, but it affects us all. In a very real world way. Most famously here in the US, we've had Russians breaking into the Democratic National Committee stealing John Podesta's emails and leaking them to try to influence the 2016 presidential election. Hacking has the power to change the course of history.

And that's why a historical perspective can shed new light on the true nature of the problem. If we take computers out of the picture, we can see things more clearly by standing back and looking at historical examples. We can look past the technology and see the underlying principles and problems. Of security and my favorite example is a cyber attack that took place in the 1830s. Yes, the 1830s on a data network built by Napoleon. From the economist. I'm Tom standage.

And from slate I'm Seth Stevenson.

Welcome to. The secret history of the future.

In the early.

1800s Napoleon built a national data network right across France and into Spain and Italy to speed up the transmission of secret military intelligence. It was based on a new technology invented by a Frenchman named Claude Chappe called the Telegraph Holder.

This is like what I think of when I think of a Telegraph, which is wires being strung along on telephone poles.

So that comes later that comes in the 1840s. So the first Telegraph and the first technology that the word is applied to is very different. It's mechanical, and it's optical. The network was made-up of lines of towers on the tops of hills about 10 miles apart from each other, and the towers were a bit like windmills with wooden arms that could be moved into different positions, and each position would signify a number or a letter. Or whatever, and to send a message, a tower at one end of the line puts its windmill arms into one particular position, and then another position a few seconds later, and so on to spell out a whole message.

So they may assume the person in the next tower down the wine who's watching through a telescope would copy the positions of the arms in sequence with the arms of his window.

That's right, and then the next tower does the same thing, and so on and so on. So the result is that the message ripples right down this line of tower. And it ends up moving in effect at about 1000 miles an hour, and that's much faster than you could send a message by horseback messenger or ship or anything like that. So for the first time you can send information faster than you can send physical objects, and this is the beginning of telecommunications. So now that you've got that ability to send symbols around and you've got 90 something possible, positions of the of the windmill arms, you can assign 26 of them to be letters of the alphabet. You can assign ten of them to be digits. You can assign some of them to be punctuation. Sometimes you might use words, and in fact one of the things they had was a. Code book and if you have the code book you understand how to interpret all of the arms weaving around, but if you haven't got the code book, it's all completely mysterious and secret. You've got no idea what any of those movements mean.

Who gets let me ask a few questions? Just establishing the system who gets to use it? Who gets to send messages?

So it's used solely to send secret. Military information and Claude Shrap, the inventor of the system, does suggest right at the beginning you might be able to use this for business purposes. Maybe you could send stock market information, he says, but that's not what it ends up being used for. Which means that if you want to send information about stock markets in Paris. Say then you have to find a way to insert your message into a government message in a way that no one will notice. And this is what our scanners did and they are the brothers, Francois and Louis Blanc. What they realized was that they. Could use. The Telegraph network. To get information about the stock market in Paris. To Bordeaux where they lived, so up until the invention of. The Telegraph, the. Fastest way to send a message was to give it to a messenger or horseback and it would take a message or horseback between three and five days to cover that distance. But now you've got the Telegraph, so you could send a message from from Paris to Bordeaux in about 20 minutes. What the bronc brothers do is they bribe somebody at the Paris end of the line to insert extra characters that indicate whether the market has gone up or down. And we don't know exactly how he did this, but it might for example be. That they inserted. You know a spurious queue in the middle of the word. If the market. Was going up and, uh, spurious, said. If it was going down and then they would immediately. Follow them with a backspace and that means at the other end of the line the message that comes out of the system is unaffected because this funny letter has come in and then it's been deleted and so the person receiving the message doesn't notice anything untoward. And then at the Bordeaux end of the line, they've got an accomplice with. A telescope who? Is a former Telegraph operator. No longer works for the Telegraph service, but still knows the code and he's looking out for this extra character, followed by the backspace character. And of course, the Telegraph towers are sitting on a hill, so anyone near the town of Bordeaux can just sit there and point a telescope at it and see what's happening and. They know the code and they know what to look out for. They can see this extra bit of information that's been slipped into the everyday transmission.

OK, so so how do they tell the person at the beginning at the Paris end of the Telegraph line what they wanted to say without getting caught?

Well, the way they did it was a little bit theatrical. They would have a glove or another item delivered to the operator at the parascender depending on the color of that item, that would specify whether the market had gone up or down. So it would look like they were just getting a series of of presents or other objects being delivered to them in the mail, and in fact this was information. Because it was encoded in the color of those.

Objects, so for an observer who's not in on the scheme, it's like that extra letter never happened. But if you've got someone who's in on the scheme then you can hijack this expensive government funded government created network for your own private purposes.

Yes, and the end result was that the blunt brothers had advanced knowledge of which way the market would move so. In effect, they could see the future in a way that rival investors in Bordeaux couldn't, and that meant they could place surefire bets on the direction of the market movement, and they couldn't lose. They started doing this in 1834 and they were soon making a lot of money, but they managed not. To draw attention. To themselves so. To other traders they must just have looked like they were very canny or. Very lucky investors.

So you're saying this is the. First cyber attack. How do you how to find that? What do? You mean by that?

This is the world first data network. It's the most advanced communication system in the world at the time it's been constructed and here we have two people who come along and make malicious use of it. They break into it and manipulate the traffic that's flowing through it for their own ends. So to me, that's a hack. That's a cyber attack.

It's sort of. Delightful that the first network in history also had the first hack in history that attacks are as old as systems and that any system that can be subverted eventually will be just because the motivations out there and people are ingenious.

This is Bruce Schneider, an expert on cryptography and computer security.

And I tend to like stories from history because they tend to be more understandable. They're less abstract than about complicated tech things, and this story is about. Windmills and telescopes and operators and simple codes. It's a lot easier to explain. I mean, you don't. Need computers to do these sorts of attacks? I mean, they're faster with computers, they're more effective with computers, but the basic ideas are the same.

Modern hacks can work in many different ways. Ransomware attacks, for example, involve computer viruses that automatically jump from one machine to another, scrambling hard disks and demanding a ransom to unscramble them. These viruses spread themselves by taking advantage of flaws in computer software. Another kind of attack is where human attackers exploit these flaws directly to gain access to a specific system so they can steal data and do bad things.

The Russian attack on John Podesta when he was chairman of Hillary Clinton presidential campaign is an example of another kind of attack. This didn't involve a virus spreading itself or exploiting a software flaw to hack directly into Podesta's computer. Instead, the Russians used a person as a way into the system because. People, all of us are. Valuable, they used a technique called spear phishing. They just sent Podesta an e-mail that tricked him.

To 2016 John Podesta, Democratic National Committee, receives an e-mail purporting to be from Google with some plausible story asking him to click on a link and login the link. Is a malicious link. It doesn't go to Google even though it looks like Google when you get to the webpage he entered in his username and password and did whatever. He had to do to log in and that went to Russian hackers and within minutes the Russian hackers used that to log into Gmail and download 10 years of his e-mail.

This kind of attack is becoming increasingly common because it doesn't involve finding subtle flaws in computer software or building viruses capable of exploiting them. Both of which are time-consuming and expensive and require deep technical knowledge. The attack on John Podesta didn't rely on there being unpatched vulnerabilities in his computer, either. Instead, it targeted the weak point where people interact with machines.

So a few years ago, Rob Joyce, who back then was the chief hacker at NSA, gave a rare public talk and what he said is that tech flaws are overrated. That the way. We break into systems is through credential stealing. And a lot of. That is based on human flaws. Most breaches these days. Have a human component.

And that was true of the blank brothers cyber attack as well, their hack relied on a technical trick inserting their own code into the Telegraph data traffic, which then spread on its own. A bit like a virus, but the way they gained access to the network was by exploiting human fallibility. They bribed people who had inside knowledge and inside. Access to the system. And this means we need to look at the bigger picture. Sure we need good technology, but to upgrade our security we also need to think about the human element too. OK, So what does that mean in practice? Well, it means we need to look beyond the way that hackers attack technology and we need to understand how they hack people.

Social engineering is. Basically convincing anyone to take an action that may or may not be in their best interest.

This is Rachel tobac. She's a white hat hacker, which means she breaks into systems, not with malicious intent, but to help identify weaknesses in security.

You can think about it as. Hacking humans.

Who are the targets? If you're trying to get into a company, how do you decide who to Go after.

I really go after the softest targets that I can find, so I'm looking for people that don't have a script. You know, if you go after somebody in customer. Support or help desk but they. Are used to denying people. Like me, they used to saying. We know that that's not in our protocol. We can't help you. So in general, I like to go after softer targets. These might be people. Like people who are within their first 90 days at the company, interns maybe younger and maybe aren't aware. Of what the protocol? Might be. Or am I trying to go after a soft but high value target? Maybe somebody like the CFO or somebody who has access to financial systems? And again, I'm going after a company because they've hired me to go after them, but a criminal. Is going to go after any and all companies. They're just going to spray. These types of. Phishing emails trying to get you to click on. A link anywhere in everywhere.

What are the typical sorts of? Tricks then it's it's. It's that sort. Of pretending to. Be clueless or ringing the help desk what? Are the sorts of things people do.

So social engineers hack through phishing, which is over e-mail. They also hack in person. We can call that like an on site attack. They'll do it over text messages, social media, or over the phone.

These techniques don't just work on non-technical people like my mum. They even work on security professionals who ought to know better. As Rachel proved when she broke into a gaming company by tricking members of its security team.

So what I did is I called them and I said hey I'm I'm traveling from my headquarters in this city and I want. To go to your headquarters. 'cause I'm giving a talk with your team and when I was there last I had my. Talk link and it didn't work at all, it was. Very stressful actually. Never loaded up. My presentation was. Just kind of. In the ether. So if you could go to my talk link and just make it sure it works on your Wi-Fi, that would be fantastic and I actually. Got two of. The High Security facility team members to open the link on both of their computers at the same time in about 30 seconds.

How would you characterize the relationship between the human factors and the technology in improving?

I think they're completely linked. We see that just over 50% of all attacks now start with a social engineering attack that we can prove. It's likely that percentage is higher, and that's just because as technical systems increase and as we see more and more sophisticated technical systems, people are going to exploit what they find might. Be easiest to exploit. Which in some cases might. Be the people of an organization.

So a lot of people I think, persist in assuming that security and network security and information security is still primarily a technical problem, and then if we just had enough technology and we had more encryption and more firewalls, everything would be fine. What do you say to people who sort of put their faith in technology like that?

I think it's good to have fantastic technology that helps protect you, but I think if you have the technology without the human element of 6. Pretty you at a disadvantage, and if you have just the human element of security without the technical systems to protect you, and whenever that human element is persuaded to do something that they might not want to do, you're also at a disadvantage. So you need. Both, it's it's. Two sides of that same coin, and. Both are needed to protect yourself.

It seems that securing our systems means recognizing that they consist of people as well as machines, and that there are vulnerabilities in both.

But the fact that.

Humans are part of the system and can make it insecure. Turns out to have a silver lining because attackers are fallible too, and very often it's human failings that lead to their exposure and discovery. Seth, let's go back to the 1830s. The first cyber attack and the Blanc brothers. They've got accomplices at both ends of the Telegraph line inserting and then extracting extra data in the flow of government, military, communications and their hack was going really well. They were making lots of.

Money, but surely the good times did not last forever, I mean. I can't help but think that if I were sitting next to a man at a Telegraph station who every day is receiving a mysterious envelope. And pulling out. Like a single Purple Glove or a single yellow glow. Of I would pretty quickly get suspicious that something untoward was happening, So what? What I'm well, first of all were. They brought down.

Where they were so it all lost it for two years and I felt pretty.

Good, it's not a time to be escalating the market.

Exactly, but then the whole scheme unraveled and the weakest point in all of this was indeed the operator at the Paris end of the line. But it wasn't because they were being sent these mysterious objects, and that sort of raised suspicions. It was because. They felt ill and the operator was worried that he wasn't going to be able to continue to do his part of the scam. So he went to one of his friends, who was also a Telegraph operator. And let him in on the secret to see if he would. Take over but that friend instead went to the authorities and then the whole hack was revealed. So the blank brothers were taken to court and this is where we look at it through modern eyes and we think come hang on a minute. This sounds familiar because it turned out that subverting the government Telegraph network was not a crime because nobody had thought to make it 1, so there wasn't any law that could be used against them. No way of punishing them. And they got away with it.

That is the best kind of crime. The crime that they haven't even realized is a crime yet.

But this is a classic example of how technology runs ahead of regulation and and so they did did introduce a crime of interfering with government telegraphs, but by that stage of course it was too late.

It was a really clever heist until it fell apart. So how does the collapse of the blunt brother scheme relate to the ways that modern day hackers get caught?

Well, the way. The blunt brothers were exposed is sort of like what happened to those Russian hackers who broke into John Podesta's computer and the Democratic National. Pity it was a human failing rather than a technical one that exposed them. In that case, the reason we know it was the Russians is that as with the blank brothers, one member of the team messed up and gave the game away. The Russian hackers were pretending to be a lone Romanian hacker and they were using something called a virtual private network to make it look as though they were in Romania. But one day one of the Russians made a fatal mistake. He forgot to switch it on and accidentally exposed the teams location in Moscow, not Romania. And that was what allowed American investigators to show that the Russian foreign Military Intelligence Agency was behind the hack.

So it basically demonstrates Bruce Schneider's point, where he said that weak points in security come at the places where humans and technology interacts.

Throughout history, people keep thinking they're going to make an unhackable system, whether it was the French Telegraph network or Enigma machines in the Second World War or blockchain today.

But they always seem to get hacked. And it turns out there's another. Example of this kind of hubris from the same era as the blonde brothers in their Telegraph.

You know there's always a way in somewhere there's always a backdoor. There's always some sort of pick or hack into into a technically designed system.

This is Doctor David Churchill. He's an expert on historical criminology and security at the University of Leeds. He studied lock picking competitions in the 19th century where lock designers would claim to have made unpickable locks and would challenge anyone to try to pick them.

The lock picking competitions arose. Basically, out of the claim by a couple of lot makers that they had invented products which could not be picked. The suggestion there being if you like that they had reached the end of a process of technical development, and therefore if you like that lawmakers should sort of give up from there or at least just find ways of making it cheaper. And easier to produce.

What on earth made? These lock designers think they could create a lock that could not be picked. That seems like hubris.

Yeah, it doesn't fit. I think there's always a temptation, particularly something. New to maybe think that you know you can create a foolproof system, or you can create something which doesn't have the kind of vulnerabilities that we use today from other things.

This was the first time that we see people claiming they had forever solved the problem of security using brilliant technology that if we throw good technology at the problem, we don't need to worry about it anymore, but they were wrong.

What was happening in the low ping competitions, obviously is that people were trying to disprove that claim and they were trying to disprove. Publicly and we were successful in doing so because, as we now appreciate, it's not possible to design so. Something that can't then be maneuvered around.

The punchline was, of course those unpickable walks got picked. We're still making that same mistake today. In the Internet era.

And we still have people building systems that they assume are secure because they can't imagine how anyone else will break into them. And this phenomenon is the key to understanding why we keep on making the same mistake. Human fallibility doesn't just apply to the users of security systems, it applies to the designers, to the people who design systems. Need to realize and accept that they are the worst at imagining how people will attack them.

They just aren't used to thinking in the surprising and devious ways that attackers do.

Right, and this concept has a name. It's called Schneider's law, named after our friend Bruce Schneider.

It is odd to have a law named after you. One of the rules I think of laws is you can't name them after yourself yourself. Other people have to do it. For you so it it kind of wasn't surprised.

Now, as law in essence states that anyone can invent a security system. So clever that. He or she can't think of how to break.

It it's the notion that I can be cleverer than everybody else combined that you know my system is is more secure, more unbreakable, less pickable, less hackable. Less guessable than anything else, right? Anybody can invent a lock that they can't pick, but you know other people might be able to.

And this explains why technology often outruns regulation too, as we saw with the Blanc brothers, regulators often can't imagine bad uses of things anymore than system designers can. And Shania law even explains. The misuse of Facebook by Russians to try to steer the election and Facebook was working as designed. Letting advertisers target specific groups of users. But the people who built it just never imagined that people would try to misuse it to swing an election.

Facebook really needed to have some evil people on its staff who be good at imagining all the nefarious things that could happen.

So this suggests we need to think about hacking in a different way and see the bigger picture. See the whole system, which includes people, all of whom are fallible, and some of whom are bad and will find ways to make unexpected and nefarious use of new technologies.

But if we're protecting ourselves against people, how do we do that? Do we just have to be suspicious of everybody?

Well, I certainly wish my mom had been a bit more suspicious when. She was rung up but. Here's what Rachel Tobac had to say.

In general, I would say be politely paranoid. Suspicious is another way. To say it, but I think politely paranoid is.

It is helpful.

For people you know, if somebody is trying to call you or e-mail you out of. The blue I. Would be politely paranoid there and reach back out to that individual with the contact information that you already had for them. I think as long as there are humans that will be human hacking, we will probably see criminals continue to attempt exploiting human human vulnerabilities. And in more and more creative ways. But I hope one day that I can work myself out of a job. Honestly, I think that would be amazing if we could train people and patch the human element of security and eventually get people to a point where they shut down every social engineering attack that would be unreal.

The common thread here is that security has just as much to do with humans as with technology, whether it's 1834 telegraphs or Victorian locks or Equifax or John Podesta's e-mail or my mum's computer. It's where people meet machines that the vulnerabilities arise. That's not something we can. Or should expect technology to fix and that's the message that's being transmitted through history hidden inside the story of the Bronk Brothers telegraphic hack.

I think it.

Shows that security is inherently a human endeavour and that people don't change. I tech might change, and tech does change all the time, but people don't, and the human factors remain constant.

I'm Tom stone.

And I'm Seth Stephenson.

The secret history of the Future is a joint production of slate and The Economist. It's produced by Bart Warshaw and Kate Holland. Editorial health was provided by Gabriel Roth, the senior producer of a slate podcast is TJ. Raphael, the executive producers are Steve Lickteig full slate podcasts and Anne Mcelvoy to the Economist.

Next time on the secret history of the future.

On one hand, this is the next step from photoshopped images that just as we had to learn not to trust photographs, now we're going to have to learn how not. To trust video. The difference being is that when we were learning to not trust photographs, we had video as a backstop. I don't know what we have after we don't trust video anymore.

Thanks for listening.