Fraudcast: stories of tricks & treachery

Episode 5: Hook, Line, and Stolen Identity

Jazz Clemente

Hello everyone and welcome to the KPMG Fraudcast, where we unravel fraud cases in the news to uncover what happened and explore lessons learned. My name is Jazz Clemente.

Frédéric LeBlond

And I'm Frédéric LeBlond.

Jazz Clemente

We're both Senior Consultants within the KPMG in Canada's Forensic practice.

Frédéric LeBlond

The stories we'll cover in this series are true events, but the names have been changed to aliases for the privacy of everyone involved. Although KPMG was not involved in these cases, we often work on cases similar to the ones of public knowledge we discuss.

Jazz Clemente

In this episode, we will be discussing the schemes used by fraudsters to get information through illegitimate means. Our stories show how these could lead to loss of finances, or in some cases even loss of life.

First, we will be discussing a story of how a phishing scheme led to a man losing millions of dollars. Two Canadian teens using aliases spoofed an Ontario Police Services email address and sent a fake news tip detailing a cryptocurrency scam to news organizations. The fake tip, which was sent to multiple media outlets, said that the local police joined forces with the FBI and the United Secret Service Electronic Crimes Task Force for an investigation. According to the police, a victim located somewhere in the US was tricked into losing $4.2 million worth of Ethereum and Bitcoin to the teens after following a link present on the fake tip shared by the media outlets.

Frédéric LeBlond

Regardless of how many security controls crypto has, one malicious link is all it takes to have millions drained from your investments.

Jazz Clemente

All your life savings gone with one click. Local police confirmed the investigation never happened, and that the email tip was not sent out by them. The story picked up local and international attention, Police said. The tip was made to look similar to legitimate media releases. Public trust in the police is valuable, and incidents like this can damage that trust.

Frédéric LeBlond

Reputational damage is one of the most difficult things to repair, and these incidents certainly do not help. This is especially impactful to the police, which depend on maintained public trust to adequately perform their duties.

Jazz Clemente

A more targeted form of phishing, spear phishing, is one of the most prevalent frauds targeting businesses and organizations. Fraudsters collect information on their intended targets so they can send convincing emails from a seemingly trusted source. Fraudsters will infiltrate or spoof a businesses or an individual's email account. Fred, can you share some variations of spear phishing attacks?

Frédéric LeBlond

Sure. Some variations of spear phishing attacks include a business receives updated payment details supposedly from an existing vendor. An accounting staff receives a large withdrawal request seemingly from their client's email. Payroll receives an email claiming to be from an employee looking to update their bank account information. Or members of religious groups receive a donation request claiming to be from their religious leader. Jazz, can you give us any warning signs we can pay attention to?

Jazz Clemente

Of course. Some warning signs include unsolicited emails, direct contact from a senior official you are not normally in contact with, pressure and unusual requests that do not follow internal procedures. It's important to remain vigilant in order to protect yourself from spear phishing. Remember to avoid opening unsolicited emails or clicking on suspicious links.

Jazz Clemente

Next, we will be discussing the story of how identity theft led a man to lose everything, including his life. John Harper was once Canada's most wanted criminal, and on Interpol's most wanted list. He was a white collar turned red collar criminal, who almost got away with everything. He thought he committed the perfect murder, but he forgot about one witness - the victim's watch. Here's how the infamous Rolex murder went down.

John Harper from Ontario had a perfect life. The married father of three started a small bookkeeping business that grew into a large financial company with multiple branches and employees.

Frédéric LeBlond

Oh, amazing. You know, I personally love when people earn their own money. This is a great start.

Jazz Clemente

It wasn't enough for him though, because it was soon revealed that he had been milking his clients to the tune of $3.2 million.

Frédéric LeBlond

Ah, I take what I said back. Big surprise.

Jazz Clemente

There's always a catch. Facing 18 counts of fraud, money laundering and theft, Harper fled to Europe in 1990, taking his middle daughter with him. John Harper made his way to England and settled in a small town under the name Aaron Allen. Harper lacked the necessary identification to obtain employment, so he jumped at the chance to enter into a business arrangement with a fellow Canadian living in England, who he had recently met. His name was Robert Scott, a television repairman. Harper used the money he embezzled to start a TV repair business with Scott. Robert Scott often spoke about his desire to return to Canada. Harper saw an opportunity and generously offered to pay for a one-way ticket so Scott could move back to Canada on the condition that he leave his driver's license, birth certificate, and a stamp of his signature back in England. This is apparently so that Harper could continue their business.

Frédéric LeBlond

Uh, don't tell me Scott accepted Harper's proposal.

Jazz Clemente

Of course, he did. Otherwise, we wouldn't have the story to tell.

Frédéric LeBlond

I don't think Scott had the chance to listen to our podcast. He surely wouldn't have done this otherwise. This is never a good idea. You're not just asking your friend to pick up your takeout for you here.

Jazz Clemente

Once Scott was back in Canada in 1992, Harper used his birth certificate and driver's license to steal his identity. In 1995, Robert Scott returned to England from Canada. Two Robert Scotts created a problem for Harper and for him there was only one solution. In 1996, he invited his former business partner to join him on a fishing trip.

Frédéric LeBlond

To return his documents?

Jazz Clemente

More like to take something more valuable. Out on the sea, Harper knocked Scott unconscious, tied an anchor to his body and dumped him into the sea. He then resumed his life as Robert Scott. Harper thought that he had gotten away with the perfect crime. The real Scott's body was found by a fisherman two weeks later. It was badly decomposed and any identification he might have had was safe with the fake Scott. What he did have on him, however, was a Rolex watch. Rolex keeps meticulous records of the sales and servicing of their time pieces, and they build them to last. The serial number on Scott's watch told police that the owner was Robert Scott. Rolex watches include the date as well as the time on their faces, and their power lasts about two days when they're inactive. Using the information from the watch, police established the time of the murder practically down to the second.

Frédéric LeBlond

And that ladies and gentlemen, is another reason why you buy a genuine watch.

Jazz Clemente

Police soon found records showing that Robert Scott was still living in England, which they found interesting since he's dead. John Harper was quickly apprehended, delighting Interpol and the Canadian government as well, but not for long. Harper was tried there for the crime and sentenced to life in prison in England, saving him from being extradited back to Canada to face his fraud and theft charges.

Jazz Clemente

Joining us for this episode as a guest is Imraan Bashir, Partner and National Public Sector Cyber Leader. With over 20 years of experience focusing on cybersecurity and information technology, including governance, strategy, incident management, cloud security, risk management, digital identity, and more. Imraan's work in this space has been recognized globally for its success as he was named one of the world's top 100 most influential people in digital government by apolitical in 2019. Welcome Imraan!

Imraan Bashir

Thanks Jazz. Thanks for having me.

Jazz Clemente

For our first question, can you explain what phishing is and how it works? What are some common techniques that cyber criminals use to execute phishing attacks?

Imraan Bashir

Yes, phishing is just honestly in layman's terms, just a way of tricking people to do something they wouldn't otherwise do. I think the most common one we see these days, and I'm sure you've all seen them in in your emails, is you get an email that you think is official, maybe it's from tax agency, maybe it's from a shipping company around Christmas is a popular one as well, and just to entice you to click a link to track your package or check the status of your tax return. But what happens is that link redirects you to something else, and that something else is a malicious site, that either gets you to download some malicious code or asks you to input a username and a password, that is then used for fraudulent purposes. Phishing can range from fake emails or fake texts, even socially engineering through a phone call where you call someone and you ask them to do something on behalf of the CEO, for example. A common one these days is getting, lower-level employees to go buy a bunch of iTunes gift cards for some reason, to pay off an invoice. These bad actors' prey on the willingness of employees to just want to do good and to want to help out. Sadly, they betray that trust by, misdirecting them somewhere else then using that to their advantage.

Jazz Clemente

What emerging trends or techniques and cyber fraud and identity theft, should individuals and businesses be aware of?

Imraan Bashir

I think the key thing that individuals and businesses need to be aware of is that this stuff changes really quickly. Five years ago, phishing emails were kind of funny in a sense in that they were in broken English, stuff was misspelled. It was really obvious that it was like, okay, I'm not going to give a bunch of money to the Prince of Nigeria here. So that's kind of the old school phishing. I think what's happened over the last few years is that it's evolved to be a lot more sophisticated, a lot more targeted, for example, administrative assistants of CEOs and really finding the right people in the companies or making sure that the email comes from a CFO and writes the email in the way that the CFO would ask for an invoice to be processed and such so that's the evolution of how it's gone so it looks more business oriented. Now, you know, speaking of where things are headed with how technology's emerging, you have stuff like AI that changing the game completely. Long gone, are those misspelled emails. Now you have very well-structured emails. You can have phishing that is done via voice now. I was reading an article the other day that a full dictionary of someone voice who's given a public speech for up to, I think five seconds or so, can have an entire dictionary clone of their voice. And then you can imagine the repercussions of using now your voice print to conduct a scam via the phone. One attack that's happened recently, and it's not related to cyber, but related to a fake kidnapping, was a bad actor taking a voice print of someone's daughter and then making a phone call to their parents to say, you know, mom, dad, I'm in Mexico, I'm in jail and something happened. I need you to wire transfer me x number of dollars to this account. As a parent, if you hear your child's voice, the first thing you want to do is make sure they're safe. You do whatever you're told. And sure enough, it's a complete scam that the woman in this case was fine at a resort and little did the parents know until it was too late. So just an example of how fast the world is evolving, misworded emails to sophisticated AI voice prompts that are going make it much more difficult, to detect going forward.

Jazz Clemente

Cyber criminals often have various motivations for engaging in fraudulent activities. Could you elaborate on some of the key motivations behind phishing and other cyber fraud schemes? Are there differences in motivations based on the type of attacker?

Imraan Bashir

There’s a broad range of attackers that are out there, whether it's a cybercriminal who just really wants to do it for financial gain to state sponsored attacks when you have governments engaging in fraud for espionage reasons, for political influence. Then you have what I call the nuisance attackers. They just want to do it because they're jerks, quite frankly. You kind of have a different range of motivation, but sadly, the impact is still the same. Generally, the impact is financial, criminal or nuisance. Even IP theft, for example, will ultimately result in financial damage to an organization. Also, I think the impact is reputational. Once you've been breached in any fashion whatsoever, it starts breaking trust between you and your customers or you and your businesses and such. The reputational damage alone can sometimes be more costly than the financial damage. Ultimately, I'll summarize by saying it varies on who the attacker is and then what they want to get out of it. But sadly, the end result for the organization tends to be very similar, either financial or reputational damage that ends up really damaging the organization in the long term.

Jazz Clemente

Onto our next topic, the concept of digital identity seems to be a hot topic around the world. Can you please explain what exactly a digital identity is and what role it might play in mitigating fraud?

Imraan Bashir

I'm a big fan of digital identity. Essentially a digital identity is an electronic representation of you. It's to prove that you are who you say you are online. I think we all know what identity means in an analog context. Like when we go, buy liquor when you're around the age of 21 or maybe a little bit older if you're lucky enough to be carded, but you have to show proof of age and when you buy a plane ticket these days you have to show proof of citizenship or whatever the case may be. You know, in the analog world, we're used to having these documents that prove who are. In the digital world, it's trickier in that we don't have electronic version of these documents, so we tend to have other representations and in the absence of a digital identity that is robust and trusted, we have this kind of mishmash of things that we show online to use as proof, but it's not exactly where it needs to be.

I think when I say digital, when I think of digital identity, I think of that analog representation in a trusted, secure fashion online. Whether it be in a digital wallet that you control as an individual that you share when you want, that you revoke consent to when you want. That is what a digital identity means to me. I think the reason I'm so passionate about digital identity is I think it can play a major role in combating or at least mitigating fraud. For example, I gave you that scenario earlier of a phishing attempt that would take you through a website to give away your username and password. In a perfect world that shouldn't matter. Like if someone got your username and password, like who cares because you have in theory, a robust digital identity behind it, and those credentials would be useless to someone because they didn't have maybe another factor of authentication. They didn't have the verified kind of proof that it is actually you behind it.

I want to live in a world where these mistakes can happen because look, we're all human. Humans make mistakes. Humans will click on links for the rest of our lives. Like that's how it will happen no matter how much we try. What I would like is a world where it's safe - we click on it and it's like, oh, I clicked on it, I made a mistake, but the impact isn't that big of a deal because we have this robust identity. I can be assured that no one can use this username and password, you know, without any additional context that I would provide with my own identity. So the extra verification levels that the digital identity will provide, the proof that it's issued by something real, like it was issued by the government and not created in someone's basement on their mom's computer, is a good start as well because these digital identities will be verified and cryptographically stamped to say, this is the official identity and that could not be replicated, you know, in a perfect world, this is my ideal world by the way that I'm describing.

What I think that'll do is make it harder for fraudsters to impersonate individuals and then give assurances to businesses, to governments, to consumers, to whoever, that you're only getting the actual information from the right source and not some fraudulent source. That's why I think digital identity will help mitigate this. The other thing I think they'll provide is full transparency. Where and when and how your identity is being used. There are some countries in Europe specifically where you as a citizen have a digital identity and you can log into your, my citizen portal and you can see exactly who queried your identity. Maybe you got pulled over by the police for speeding - you would get home, you would look at your portal, you would say, at 1:15 PM, this identity was queried for this purpose.

You would have full transparency to how and why your identity is being used. What I think that does is actually enhance privacy that you can kind of see what's happening. You have assurance that it's being used for the intended purpose, and nothing more as opposed to today when we have no idea who's got a copy of our driver's license or passport or whatever, who knows what's happening behind the scenes right now and usually only find out when it's too late. In summary, I think digital identity helps kind of prevent and detect and therefore helps you respond to any sort of theft or fraud in the future.

Jazz Clemente

What are some of the risks or challenges in implementing a digital identity in Canada?

Imraan Bashir

I know this one very well because this was my old job actually prior to joining KPMG. Canada's an interesting country in that we are a federation, right? We have provinces and territories that have jurisdiction over some elements of identity. We have the federal government, particularly immigration, the immigration department that has some pieces of identity. The challenge that we have compared to maybe some European countries that have more centralized governments is that our data is literally all over the country. We need to create an ecosystem of identity in this country where there is interoperability. You know, for example, I was born in Ontario, therefore my root identity, the fact that I was born here, my birth certificate was issued by the registrar of Ontario.

My parents immigrated here. When they became permanent residents, first that permanent residency was issued by immigration, which then led them to get a passport and then a driver's license and such, so that these other pieces of identity were derived from that first piece. You can see that the ecosystem is a bit of a complex web. For digital identity to work properly in this country, we need all levels of government to interoperate one another and share this data willingly and with consent of the individual as well. I think this is why it's been so difficult to get it running in this country as opposed to other ones, not to mention the vastness of our country. I would also say the seriousness of the privacy concerns. I think there's no question our country's very adamant about how important our privacy is and rightfully so. I'm also very conscious of the fact that we need to make sure we get this right. This is not a system you can pilot and hope for the best. We mess this up, we lose trust with our citizens and that's not going to bode well over time. I think it's really important, and I know a lot of the homework that's being done or has been done over the last decade is related to how do you implement this right the first time? How do you make sure that users are in full control, fully consent, can fully revoke at any time, have full transparency and that data is minimized and you can select just the bare amount of data you want to share with an entity and nothing more. That is why it's been taking so long.

In my heart of hearts, I think that is the right move to make sure that when we implement it, it's implemented in a responsible fashion as opposed to there are some implementations around the world that are more authoritarian and maybe have collected a bit more data centrally than per se I would like as a cyber guy and as proponent of privacy. So long-winded answer to say that there's a lot of challenges here in Canada. We have a lot of smart people working on it, and I'm optimistic that it's something we can solve in the near future.

Jazz Clemente

Wow, that was really interesting. Thank you so much for joining us, Imraan.

Imraan Bashir

No problem. Thanks a lot for having me. That was fun!

Frédéric LeBlond

Each episode we'd like to leave you with a little something to help increase fraud awareness. Here's Jazz with our fraud scheme of the week - Identity theft.

Jazz Clemente

Are you having trouble signing into your online accounts? Are things looking different when you log in? Are there unfamiliar charges on your bank card? Did your credit score suddenly drop? These may be signs that your identity has been stolen. Identity theft is the crime of obtaining the personal or financial information of another person. The stolen identities are often used to commit fraud, such as making unauthorized transactions or purchases. Identity theft victims are typically left with damage to their finances and even their reputation. There are two major kinds of identity theft. In traditional identity theft, a fraudster takes over someone else's identity and uses stolen documents for the fraud. They usually max out the credit immediately, which alerts the victim about the fraud. This identity theft gets reported more quickly than a synthetic one. On the other side, victims of synthetic identity theft are not as quickly alerted since a combination of fake information and real information is used. For example, fraudsters can combine wrong information with social insurance numbers and names to make a new identity and carry out financial crime.

Frédéric LeBlond

Jazz, how do we manage this?

Jazz Clemente

There are several tips to remember to minimize your risk of being a victim of identity theft. Reduce the number of items with personal information you carry around with you. Check your mailbox in a timely manner. Shred any documents with your personal information before discarding. Be aware of telephone online or door-to-door solicitations, which claim to be legitimate entities. Keep your financial documents, credit cards and blank checkbooks in a secure location such as a safe. Pay attention to billing cycles for statements that do not arrive in the mail. Use a secure internet connection online when entering and transmitting personal information and be reluctant to register with websites that request your personal information.

Frédéric LeBlond

KPMG Forensic professionals transform how clients identify, mitigate, and respond to risk saving time and money. We help individuals and organizations stay on top of fraud, and we would love to help you too. On behalf of the whole KPMG in Canada Forensic team, thank you very much for tuning into this episode of the KPMG Fraudcast.

Jazz Clemente

And we hope you join us again next time.