International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 11 Issue 10, October- 2021
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Security from financial frauds: online and offline

Yogesh Gautam
Pr. Scientist
ICAR-Directorate of Mushroom Research
Chambaghat, Solan Himachal Pradesh, INDIA
Yogesh.Gautam@icar.gov.in

India recorded 50,035 cases of cyber crime in 2020, an 11.8 per cent surge in such offences over the previous year, according to the National Crime Records Bureau (NCRB) data.**There's very little that can be done aboutcyber crime at your end, apart from being more vigilant. But certainly there are different actions which can be taken, which can make a lot of difference.**The Reserve Bank of India (RBI) has time and again cautioned bank customers of fraud, including those in Know-Your-Customer (KYC) cases.

'V-Shaped Growth for Economy

In fact, certain frauds have become more prevalent than others, and being aware of them is the first step towards protect yourself.Mayur Joshi, chief executive officer, Indiaforensic.com, a company engaged in the prevention, detection, and investigation of frauds says, "It is necessary to learn, to read about these scams."

Here are some such frauds, their methods and what can be done to avoid them.

K**YC Fraud:** Due to the pandemic, many people stopped visiting bank branches, providing fraudsters an opportunity to use KYC as a reason to engage with customers by pretending to be bankers.

The modus operandi is simple."You get an unsolicited SMS saying your card or account will be blocked, or rewards points will be disabled--the kind of message that creates panic in the customer.

"And that customer naturally reacts to the SMS, without considering the legitimacy of the message."

Once you call the number mentioned in the SMS, they entice you for personal details under the pretext of KYC verification.

For instance, you will be asked for account or login details, card information, PIN, OTP, etc. Bhatia says, "They may also ask you to install a remote access app, which will give them complete access to your mobile."

The fraudster quickly cleans the account empty, while the victim keeps getting SMS of the amount debited from the account.

What to do: Remember the KYC update will never happen via a third-party app.
Bhatia says, "You should get in touch with the bank or card issuer--not on the number in the SMS, but the one on the reverse of your card--or call your bank customer care."
Don't even go by web-searches, as fraudsters are also spreading fake customer care numbers of banks or UPI platforms online.

YashTyagi, chief technology officer (CTO) CASHe, says, "Be very careful to whom you give out your information or documents for KYC purposes as well, even if you are doing so on a website.
"There are many fraud sites that collect such data. Fraudsters can make copies of KYC data and use it to apply for loans."

So it's not just SMS, calls or email you should be wary of, but websites as well.

Sim Swap Fraud: Swap simply means exchanging one thing for another.
Let's say you have a 3G SIM card and want to upgrade to 4G.
You request a swap 3G SIM for a 4G SIM from the service provider.
This is an authentic SIM swap. Here you are putting the request to your service provider who deactivates your old SIM and gives you a new one, which activates within a few hours.
Our mobile phones are loaded with information, right from contact lists, photos, emails, and SMS to financial details such as ATM withdrawals alerts and one-time passwords sent by banks for net banking transactions.
Joshi says, "The SIM Swap fraud is a nightmare that many mobile holders faced during the pandemic.
"Many users were locked in when they started receiving messages that their SIM card has been blocked or the request for changing the SIM had been received."
Fraudsters use SIM swap techniques to steal your financial details by blocking your SIM card and exchanging it with a fake one.

Joshi says, "The swapsters approach the service provider (posing as a genuine card holder, with fake papers), requesting to swap the SIM.

"After verification, the service provider deactivates the old SIM.

"The fraudsters get a new active mobile SIM card."

This means once the SIM is swapped they get access to your OTPs, financial accounts and card related alerts, which they used to commit the fraud.

Before contacting a service provider, the fraudster will usually engage in some form of social engineering to try and gain information about their intended victim that can be used to answer security questions related to the victim’s mobile number.

Joshi adds, "This can be done by researching the victim’s social media accounts or gathering information about them from other public sources.

"The person attempting the SIM swap might also send phishing emails to a potential victim in the hope of obtaining other sensitive information that can be used to unlock his mobile phone number."

Phishing is a kind of e-mail fraud technique in which the crook sends out genuine-looking emails or website links in an attempt to gather your personal and financial information.

What to do: Don’t give away your details to anyone.

If you see no service on your SIM, contact the service provider at the earliest.

If your SIM has been deactivated at midnight, you can’t do much about it, really.

UPI-related Frauds: Unified payments interface (UPI) has a feature in which you or the merchant can send the user a request to collect money.

This feature is being used by fraudsters on second shopping websites.

Manoj Chopra, head, innovation & product development, InfrasoftTech says, "When you try to sell an item on such a site, fraudsters feign interest in buying and send you a collect money request instead of sending money.

"Remember, you don't need to authorise a transaction if the money is being transferred to your account, but the fraudster makes you believe you do and you end up sharing the PIN, and your hard-earned money gets re-routed."

What can you do: Remember when you are receiving money in your bank account you don't have to give a PIN or OTP.

Likewise when you are receiving money in UPI you don't need to enter any PIN.

Treat your PIN exactly like you treat your ATM PIN. Don't disclose it to anyone.

Offline Frauds: Oftentimes we take cash withdrawal from an ATM casually, not realising that a little carelessness could cost us our hard earned money.

Shoulder surfing is such a danger associated with ATMs.

Shoulder surfing is, in simple terms, when someone stands close to you or at a very close distance in order to get information.

Chopra says, "So, while using an open ATM, be careful that nobody is shoulder surfing you. You can never tell whether or not the person shoulder surfing is a fraudster.

"Such people stand close to you to get the personal identification number (PIN) of your card while you are feeding it."

Once your PIN is compromised, it can be used by fraudsters in ways you can't even imagine.

Chopra says, "He could also have tampered with the ATM, by inserting a device in the ATM card slot.

"So, when you punch your PIN, the device captures the number and other information stored on your card."

Fraudsters who use the data to make cloned cards and withdraw cash at overseas ATMs, or shop online.

What can you do: First, look closely at the card slots in the ATMs.

Ensure that there ae no parts jutting out, no broken pieces, no cracks or any glue-like substances around the slot.

It's a good practice to cover the hand while punching your PIN on the key.

Also make sure no one is shoulder surfing.

Things to keep in mind: There’s very little you can do at your end, apart from being more vigilant.

But some things that you must do can make a lot of difference. First and foremost, follow the basic online security hygiene against phishing. (See box).

Ankit Ratan, co-founder and CEO, Signzy, an AI-based banking workflow automation solutions provider, says, "Use the facility that allows you to set and modify transaction limits on your cards and savings account.

"That way, you will be able to reduce the risk considerably."

You can set limits on all types of translations--domestic, international, POS, ATM withdrawals, and online.

Banks also allow you to switch on and switch off your debit and credit card.

Imagine the peace of mind when you temporarily switch off a card you aren't using and set a limit one those that you use.

This way at least some damage will be next to zero.

Use robust passwords which is a non-word with multi-factor authentication and make it long.

Cyber Law

Law in cyberspace isn't the same as law in the real world. Some real-world legal frameworks don't work as well as they could when they get extended to the Internet. The law of war, as defined by the four Geneva Conventions and the three Additional Protocols, is a good example of this.

The Geneva Conventions provide a framework under which many nations have agreed to fight wars. They specify what ways are OK to respond to an armed attack and which ways aren't. Note that's "armed attack," not "act of war." Armed attacks are what the Geneva Conventions talk about. Acts of war are what politicians talk about to score political points.

When politicians say that their country will treat a cyber-attack on it as an act of war, that's an intentionally vague statement that doesn't really mean anything. Treaties tell you how you can respond to armed attacks; they don't say anything about acts of war. So the right question to ask is whether or not cyber-attacks count as armed attacks, and how cyber-attacks can be understood within the framework that existing treaties provide.

The Tallinn Manuals

Representatives from the NATO countries did a thorough review of this question and published their results in the Tallinn Manual (2013) and the Tallinn Manual 2 (2017), both named for the city in Estonia where the projects were based. (A Tallinn Manual 3 is in the works and should be published in 2026.) What the original Tallinn Manual found, roughly, was that if the effects of a cyber-attack are comparable to a conventional ("kinetic") attack, then it counts as an armed attack and the existing law of war gives a framework for acceptable ways to respond.

Unfortunately, this doesn't cover most cyber-attacks. Kinetic attacks destroy things; most cyber-attacks don't. If you're hit by ransomware, the effects are very different from those of a cruise missile hitting one of your data centers. In one case, your computers are destroyed; in the other, they just need to have software reinstalled. And because the effects are so different, it's not clear that the existing law of war tells governments what are and are not acceptable ways to respond to cyber-attacks unless they cause serious physical damage.

Such attacks are rare. The 2014 cyber-attack on a German steel mill is one of the few instances. The Stuxnet worm of 2010 is thought to have had the objective of damaging Iranian centrifuges, but an analysis of Iranian purchases of centrifuges over time suggests that they did not increase after Stuxnet was released. So Stuxnet might not have caused any significant physical damage. (Although it's possible that maintenance issues with the Iranian centrifuges were so serious that they hid any damage caused by Stuxnet.)

The Tallinn Manual 2 tried to extend the Tallinn Manual’s interpretation of the Geneva Conventions to attacks that are less damaging than an armed attack. It doesn’t seem to do as useful a job of this as the first Tallinn Manual did. The first manual addressed a black-and-white issue, but the second set out to examine several shades of gray, and its conclusions are just as gray: "Maybe, maybe not" is one way to put it, but you could also say “It depends" or "Possibly.” I could have told you as much without a multi-year effort involving hundreds of people from dozens of countries.

It’s not clear how useful the Tallinn Manual projects were. They might reflect a minority opinion that doesn’t really matter. Only NATO nations were involved in writing the Tallinn Manuals, so lots of countries—including China, Russia, Israel, Iran, and North Korea—that probably have significant cyber-war capabilities didn’t participate. The NATO countries may think that a particular interpretation of the Geneva Conventions is valid in cyberspace, but if their adversaries there don’t see the same rules as applying, then it’s not clear how useful the Tallinn Manuals are.

But the Tallinn Manuals might still be useful in some ways. Most countries aren’t as powerful as the NATO countries or the other countries with significant cyber-war capabilities. If a cyber adversary decides to attack them, they don’t have the ability to retaliate like the stronger countries do. The best that most countries can hope for is that the more powerful ones generally follow the rules that treaties specify. From that point of view, the Tallinn Manuals might provide a reasonable way for less powerful countries to know what they should generally expect from the more powerful ones, even if the powerful countries don’t always follow the rules.

Rules of space combat are key

Game theory tells us that it’s probably not possible to get all nation-states to agree to not develop cyber weapons for use in space. The situation resembles that of nuclear weapons—the first state to cheat wins, so a rational government would never agree to eliminate nuclear weapons. But if we can agree to a reasonable set of rules that nations need to follow for space combat, that would probably be to everyone's advantage.

There are good reasons for national governments to want to gain control of space. Let's see if the Woomera Manual and MILAMOS are good steps in that direction. They might create a useful legal framework within which to confine future cyber operations.

Why safe harbour is the best way forward for data protection

Data breach notification laws have become popular among the states—all 50 have them—as well as in the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. Once these measures are on the books, though, states continue to tinker with them. This year, for example, 22 states in the USA have introduced or considered bills amending existing laws.

Many of the alterations focus on changing the time required to report a breach, expanding who needs to report a breach, redefining what's considered personal information, and requiring reporting of breaches to the attorney general or another regulator in the state.

Some states are considering providing incentives for organizations to beef up their security by providing them with an affirmative defense in civil lawsuits if it can be shown that reasonable security practices were in place at the time of a data breach. Motivating organizations to address data privacy can be difficult. Hence, the incentive.

Here's why incentivizing data protection with so-called safe harbor provisions is the best approach to bolstering cybersecurity.

Safe harbour for meeting standards

Unlike the punitive approach adopted by states such as California and Colorado, states using the incentive approach try to encourage higher levels of cybersecurity by creating a "safe harbor" from data breach litigation by implementing industry or government security standards.

This year states considering bills with affirmative defense provisions include Georgia, New Jersey, Illinois, and Connecticut. Nevada rejected a measure that would have provided immunity from liability for damages if certain security controls or standards are in place. Meanwhile, a measure establishing an affirmative defense was enacted in Utah.

The Cybersecurity Affirmative Defense Act (HB80) is an amendment to Utah's data breach notification law, creating several affirmative defenses for persons facing a cause of action arising out of a breach of system security, and establishing the requirements for asserting such a defense.

The basic intent of the act is to prod individuals, associations, corporations, and other entities to maintain reasonable safeguards to protect personal information by providing an affirmative defense in litigation flowing from a data breach. The incentive is that a person who creates, maintains, and reasonably complies with a written cybersecurity program that is in place at the time of the breach will be able to take advantage of an affirmative defense to certain claims under the act.

The act does not provide any affirmative defense if the person had actual notice of a threat or hazard to the security, confidentiality, or integrity of personal information; if the person did not act in a reasonable amount of time to take known remedial efforts to protect the personal information against the threat or hazard; or if the threat or hazard resulted in the breach of system security. These exclusions are a reminder that a cybersecurity program is not a “write it and forget it” exercise. They put organizations on notice that cybersecurity programs are a risk management tool for a business entity.

Utah isn't alone in establishing an affirmative defense to claims arising from a data breach. Back in 2018, Ohio enacted the Ohio Data Protection Act (SB 220), similarly providing a safe harbor for businesses implementing and maintaining "reasonable" cybersecurity controls.

In a "client alert" published at the time the Ohio law was enacted, the law firm Franz Ward explained that to qualify for the defense, a business must implement written cybersecurity measures designed to protect the security and confidentiality of personal information, protect against any anticipated threats or hazards to the security or integrity of the personal information, and protect against unauthorized access to and acquisition of information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

Beyond that, a covered entity’s cybersecurity program must “reasonably conform” to one of several industry-recognized or regulatory frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework, the Federal Risk and Authorization Management

Program, the Security Rule of the Health Insurance Portability and Accountability Act, or the Payment Card Industry's Data Security Standards, among others.

Protections are good but limited

The law's protections are noticeably limited in scope to certain types of tort claims, leaving even those businesses that have robust cybersecurity programs vulnerable to statutory violations, such as data breach notification requirements, or claims based in contract, such as a business-vendor dispute.

New York has a similar but narrower version of the Utah and Ohio statutes. Enacted in 2020, New York's Stop Hacks and Improve Electronic Data Security Act requires that organizations that collect data maintain reasonable security, according to applicable regulatory schemes—such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, which requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data—and also specific agencies such as the New York State Education Department and its Department of Motor Vehicles.

High-maintenance moves

This analogy isn't perfect, but changing software with a search warrant seems a bit like using a warrant to search a 2015 Toyota and somehow turning it into an unmarked 1987 Yugo. Maybe the other way around, if you're lucky, but things never seem to work out that way.
In that hypothetical exercise, the authorities didn't just search the car for evidence that might be used to investigate illegal activities. Instead, they also changed the car into a different one.
I'm not a lawyer, but it's not clear to me that that's within what's allowed for a search warrant. And if that unmarked 1987 Yugo costs more to maintain, the owner has a good reason to not be happy. In that case, who would be responsible for the higher maintenance costs?

Our work is never done

If you're a developer, you know that software is never completed. Instead, it's just deemed good enough for the upcoming release. I've never done software testing, but testers tell me that it's about the same: You never have enough time to test everything, so you make a commercially reasonable effort to test the most important features of your product.

But with the patch to this hack of Exchange Server, how much testing did the FBI do? Would it even count as “commercially reasonable” if a software vendor did it? Perhaps not. It looks as if it was deployed too quickly for that to have taken place. And it probably wasn’t tested in the environments that the users of Exchange Server were running in, making unexpected interactions more likely. Do you really want someone installing relatively untested patches to your software? It looks as if that might be what the FBI did in this particular situation.

Unwarranted patching?

To obtain a search warrant, you need probable cause that a crime has taken place. The warrant application for this particular situation says that the FBI identified certain Exchange Servers that were compromised. Its justification of probable cause is the fact that “these victims are unlikely to remove the remaining web shells because the web shells are difficult to find due to their unique file names and paths or because these victims lack the technical ability to remove them on their own.”

The FBI noted that by “deleting the web shells, FBI personnel will prevent malicious cyber actors from using the web shells to access the servers and install additional malware on them.” But is that a good reason to justify a search warrant? My understanding of search warrants is that they are used to gather evidence that can be used to prosecute criminals, not to patch software, even if there is a very good reason for that patch to be installed.

Conclusion

So even though the government’s intentions seem to have been good, in some cases, it’s not clear that whether it was a proper use of a search warrant. Requiring search warrants is an important protection of our privacy, and we should be concerned when the government extends its ability to do searches in ways that seem to be an innovative interpretation of the law. This seems a good example of a case that we should worry about.We will have to accept that extending our existing framework for limiting the government’s ability to do searches will need some modification when it’s extended to cyberspace, but I’m not sure that what the FBI did in this particular case is the right way to do it. Even a perfectly valid goal shouldn’t justify any means of attaining it.