RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF JURIDICAL SCIENCES

COURSE NAME : BALLB/BBALLB

SEMESTER : VIIIth

SUBJECT : Banking law

SUBJECT CODE: BAL -802/BBL-802

LECTURE : 25

FACULTY NAME: Mr JP Srivastava

Banking thefts

Online banking is the norm for most people, with around 30% of people now using a digital-only bank. Unfortunately, this means that online banking theft is also on the rise. Sophisticated digital gangs are always looking out for weak spots, causing misery for their hapless victims.

Banking online doesn't have to be dangerous, as long as you understand the threat and take steps to protect yourself. Here's what you need to know.

8 ways online banking thieves will try to steal your money

Banks are always working to improve security, but hackers and fraudsters are highly inventive. They will exploit any potential weakness that grants access to your cash.

There are some attack patterns that we see again and again. Here are eight to watch out for.

1.Phishing emails
Phishing emails look like legitimate emails from your online banking provider. Some phishing emails are so professional-looking that even an expert might think that they're the real thing. The email will often claim that your account needs urgent attention.

If you click the link in the email, you'll find yourself on what appears to be your bank's official website. This website will ask you to enter your security details and might also ask you for other information, such as your card details or your PIN. Any information you enter on this phony website will go straight to the scammers, who will then log into your real online banking account.

2.Fake website attack

Just like a phishing attack, this technique guides you towards a counterfeit version of your bank's website. The twist in this version is that not only is the website fake, but the browser is also fake.

Hackers perform this attack with a trojan—a type of virus that sneaks in and installs itself on your computer. When you try to access your bank, the virus creates a pop-up browser window that looks just like the real thing. You enter your details into the fake website, but instead of logging in, you're sending your information straight through to the online thieves.,

3.Keylogger trojans
A keylogger is the online banking equivalent of someone looking over your shoulder at the ATM. This type of trojan virus allows hackers to see everything you type on your keyboard, including your banking password and answers to challenge questions.

Hackers have many ways of tricking you into installing a keylogger, often through an infected email or website. Once a keylogger is on your device, your keyboard is broadcasting directly to the criminals. They just need to wait for you to type your login details, and then they can take over your account.

4.Stolen passwords

Occasionally, a large company will reveal that they've experienced a data breach. This means hackers have obtained access to sensitive customer details, which can often include usernames and passwords. Hackers usually sell these details to criminal gangs, who then pursue large-scale fraud campaigns.

Breaches are a nightmare for people who use one password on every website. When you always reuse the same password, it's like creating a master key that opens every door. If someone breaks into a less secure system, they'll get hold of your master key, which they can use to access all of your accounts – including your online banking.

5.Insecure wi-fi

We often hop between wi-fi connections without even thinking about it. When traveling, for example, you might jump on any available free network. But this means that you have no idea whether you're on a secure connection. If it's not, hackers can exploit this vulnerability to read your outgoing data.

Some cybercriminals go a step further and create their own fraudulent wi-fi networks. You might think you're connecting to COFFEESHOP_Free, but in actuality, you're connecting to a stranger's wireless router. They can then monitor any traffic that passes through their network – including your login details.

6.Text message spoofing

Most banks rely on SMS to send account updates and urgent alerts. Smartphones often combine these conversations, so you can see all incoming messages from your bank in a single thread. This means that if someone can spoof your bank's phone ID, there's almost no way of knowing that you're looking at a fake message.

This attack works on the same principle as phishing. Fake text messages will direct you towards a fake website, which will then try to capture your login details. Often, there's very little to suggest that you might be looking at a fraud.

7.DNS cache poisoning
DNS is the system that allows your browser to find its way around the internet. When you type an address—such as Kaspersky.com—your browser looks in the cache to see if you've ever visited that site before. If so, it will know which IP address to visit and take you right there.

Cache poisoning is a sophisticated technique that drops a malicious IP address into your system. It usually happens when you visit a malware site, even briefly. If a poison IP

reaches your DNS history, your browser will take you to the fraudster's website next time you try to access your bank.

8.Social engineering attacks
Fraudsters have endless ways of tricking people into revealing their banking details. They might call and pretend to be bank employees, or they may browse your social media to find answers to your security questions. This is known as social engineering.

Another approach is to simply ask you to send them money. Cybercriminals often employ the advance-fee scam, in which they promise to send you a large reward if you pay an upfront amount. Once they have your fee, they disappear. They might also make up stories about personal difficulty and ask you for financial help.

6 signs of online banking theft to watch out for

Online banking security is almost as robust as the security in a bricks-and-mortar bank. That's why cybercriminals rarely try to attack the bank directly.

Instead, they focus on you, the customer. As you've seen above, the most common type of attack involves tricking you in some way. The goal is to either steal your details or plant a virus on your device.

There are some tell-tale signs to watch out for. Be alert if you notice any of the following:

Absence of personal details

Does the email say 'Dear customer' rather than 'Dear [your name]'? If so, it may well be a scam. Many online banks will include some personal details in their communication. This is actually a security measure to help you recognize legitimate messages.

Requests for secure information

Banks will never ask you for certain details, such as your PIN. However, scammers will try to get as much detail as possible, such as your username, password, phone number, and answers to any security question. They need these details so they can pretend to be you and access your account.

Invalid security certificate

Genuine banking websites have a security certificate. You can see this in your browser: right next to the URL, you should see a padlock browser. Click on this padlock, and you'll see a confirmation of the site identity. For example, if you click on the padlock for this website, for instance, you'll see that it's registered to kapersky.com. Fake websites do not have a valid security certificate.

Instruction to download file or install software

Most financial institutions won't send you invoices or statements as email attachments. Instead, they'll ask you to log in and view your documents securely. Criminals may try to disguise virus installers as downloadable attachments. They may also ask you to install software, often claiming that this software is required to protect your account. You should only ever download and install software from certified sources .

Unusual URL or email address

The scammer's email address or website URL will differ slightly from your bank's site. Sometimes the difference might be subtle, like an additional hyphen, or an uppercase I in place of a lowercase L.

Sense of urgency

Fraudsters will always try to rush you. They may pretend that your account has been hacked or that you've missed a payment. Their goal is to make you panic so that you act without thinking.

Banks want to keep you safe, so they will always encourage you to put security first, even when your account requires urgent attention. Take time to learn about your bank's security protocols. This knowledge will help you stay safe and avoid criminals.

Practical things you can do to protect yourself from online banking theft

Even if you avoid all social engineering attacks, you could be vulnerable. Digital thieves will try to get into your account any way they can. Here are a few ways to toughen up security.

- **Activate two-factor verification: 2FA, or two-factor authentication, adds an extra step to the login process. Usually, this involves sending an SMS to your registered phone number. You'll need to enter this security code before you can access your account. You may be able to use an authenticator app such as Google Authenticator to generate a login code.**
- **Secure your devices: Install a powerful anti-virus on your desktop, laptop, tablet, and phone. Make sure that you choose an anti-virus service that automatically updates to protect against the most recent trojans, malware and spyware.**
- **Defend your browser: Install a browser add-on that warns you if you're about to visit an unsafe website. This program will flash up a warning before you visit a site that's known to contain active security threats, such as viruses or malicious cookies.**
- **Use a VPN: A Virtual Private Network (VPN) encrypts all of your traffic end-to-end, even when you're on public wi-fi. If someone intercepts your data in transit, they won't be able to obtain any sensitive details.**
- **Encrypt financial transactions: When buying online, you may expose your bank or credit card details. This potentially exposes them to malicious programs like keylogger trojans. Use a payment protection tool to encrypt purchases and other transactions.**
- **Scan attachments before opening: Email attachments are often unsafe, even if they're from someone you trust. Hackers may have gained access to the sender's account,**

and they could then send malicious emails to others. Scan any attachments with an anti-virus before you open them.

- **Use a password manager: Password managers create unique, hard-to-crack passwords for every site. When you want to log in, the password manager will auto-fill your details, so you never have to worry about forgetting your details. You only need to remember the login details for your password manager.**

Recommended products

- **Kaspersky Security Cloud**
- **Kaspersky Total Security**
- **Kaspersky VPN Secure Connection**
- **Kaspersky Password Manager**

MCQs

1. The relationship between a banker and customer is.....

a) That of a debtor and creditor

b) That of a creditor and debtor

c) Primarily that of a debtor and a creditor

d) (a) and (b) together

2. The banker has a lien on.....

a) Bonds given for collection

b) Bonds given for safe custody

c) Bonds left by mistake

d) (a) and (b) together

3. In executing the standing instructions, there exists a relationship of.....

a) debtor and creditor

b) Trustee and Beneficiary

c) Bailee and Bailor

d) Agent and Principal

4. To constitute a person as a customer.....

a) There must be frequency of transactions

b) There must be a dealing of a banking nature

c) There must be some sort of an account

d) There must be a single transactions of any nature

5. The banker has a statutory obligation to.....

a) Honour customers' cheque

b) Exercise lien

c) Maintain secrecy of his customers' accounts

d) Honour customers' bill