TOPIC: Digital Payment Awareness

COURSE: CCC Concepts

DAY: 43

NIELIT

Presented By: Anjali Dhingan

Safety Precautions

DIGITAL FINANCIAL SERVICES

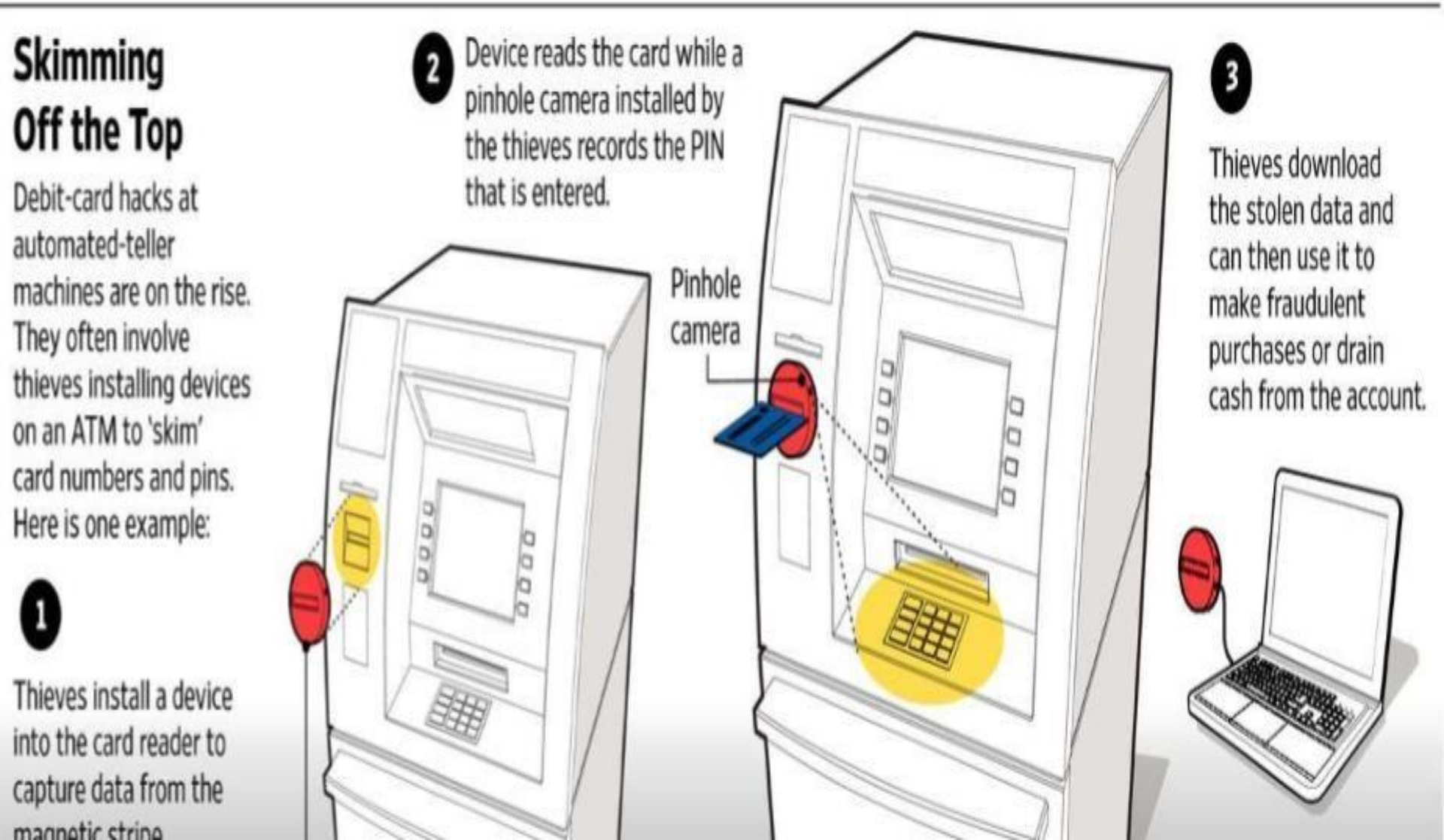
Safe and Secure Banking Tips

- Always use genuine anti-virus software
- Avoid using public Wi-Fi or Use VPN Software
- Check for latest updates of Operating System
- Change your password regularly and ensure that it’s a strong one
- Don’t use public computers to login to net banking
- Be Aware of skimming (where fraudsters install a device on top of card reader in ATM machine

Safe and Secure Banking Tips

- Always check the last log-in date and time, in the post login page
- Never store User-id and Password in written somewhere
- Avoid Signing-in to your net banking account via phishing mailers
- Don’t share your OTP through call or email
- Use only the official bank app provided by Google play store
- Ensure correct URL https:\ and any other tracking cookies

Skimming


Skimming Off the Top
Debit-card hacks at automated-teller machines are on the rise. They often involve thieves installing devices on an ATM to 'skim' card numbers and pins. Here is one example:
1
Thieves install a device into the card reader to capture data from the magnetic stripe
2
Device reads the card while a pinhole camera installed by the thieves records the PIN that is entered.
Pinhole camera
3
Thieves download the stolen data and can then use it to make fraudulent purchases or drain cash from the account.

Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit/debit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication

Using Botnets

- Botnets are computers infected by worms or Trojans and taken over surreptitiously (secretly) by hackers and brought into networks to send spam, more viruses, or launch denial of service attacks

- Remotely controlled by the attacker.
  - SQL Injection attacks

Keyloggers

- A keylogger (short for keystroke **logger**) is software that tracks or logs the **keys** struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored
- Modified to extract personal information
- Keyloggers are designed to monitor all the key strokes

Few Useful Tips

- Use a power-on/access password for your computer, laptop and mobile as well as a screensaver password so that no one else can access your systems without consent
- Change your passwords and security settings regularly
- Always visit your bank's secure Internet Banking site directly
- Avoid accessing the site through a third-party link or via email
- Verify the domain name before you try to log in

Few Useful Tips

- Log out of your Internet Banking account the minute you complete transactions; Do not close the window without logging off
- Avoid using Internet Banking on unsecured Wi-Fi networks such as railway stations, airports and cybercafés
- Install authentic security programmes to guard your system and account against hackers, virus attacks and other malware
- Update the security programme or antivirus regularly

Few Useful Tips

- Install a suitable firewall to protect your computer or laptop and its contents
- Never provide remote access to your system to anyone; not even family members, as it is still vulnerable to hacking
- Disable the ‘File and Printing Sharing’ command on the operating system
- Always log off your PC or laptop when not in use; don’t keep it lying around or trust a stranger with it

Few Useful Tips

- Never save your mobile banking log-in and password on the phone; memorize it
- Never leave your handset unattended and logged into a mobile banking app
- Always lock your phone to prevent unauthorized use
- Notify your bank as soon as your mobile is lost or stolen
- Update the mobile banking app as and when a new version/upgrade is released

Few Useful Tips

- Update your phone with latest security patches
- Never download apps from untrustworthy and dubious sources
- Always log out of your banking app after using it
- Keep an eye on your account balance and transaction history regularly
- If you suspect unauthorized transactions on your account, report it to your bank immediately

Thank you!