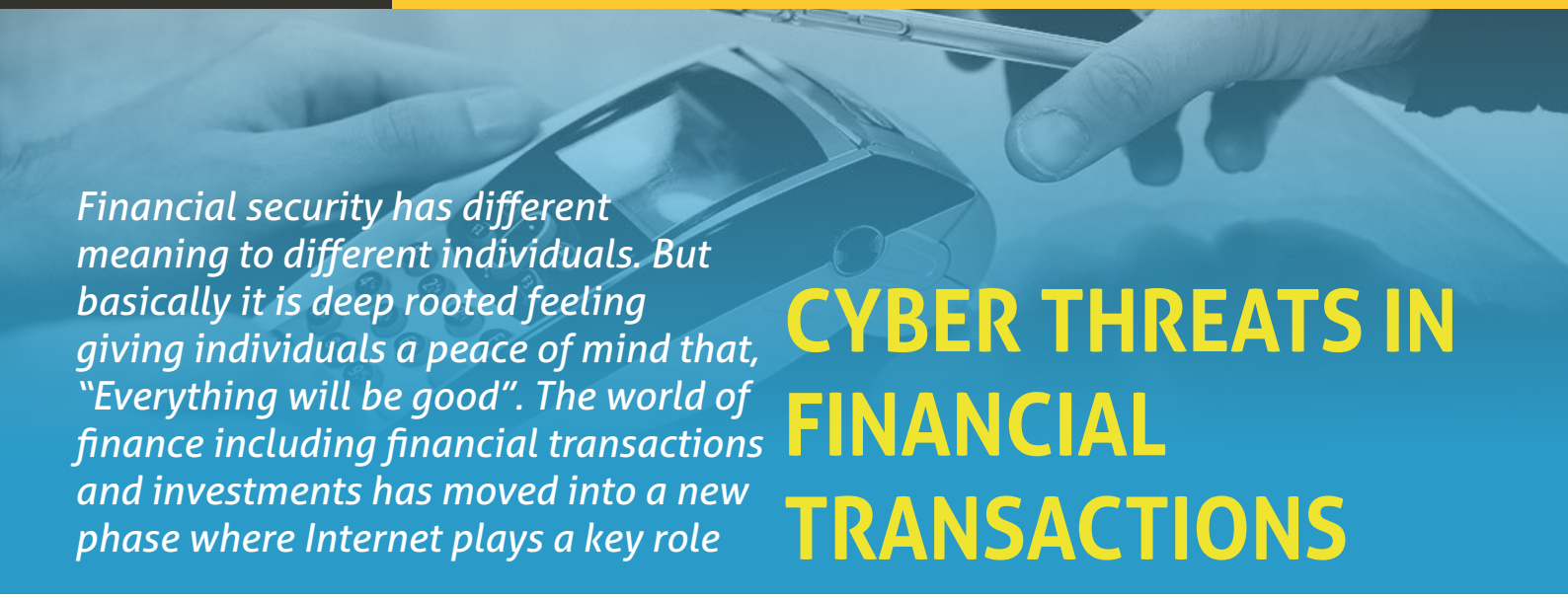
InfoSec Newsletter

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2020



Financial security has different meaning to different individuals. But basically it is deep rooted feeling giving individuals a peace of mind that, "Everything will be good". The world of finance including financial transactions and investments has moved into a new phase where Internet plays a key role

CYBER THREATS IN FINANCIAL TRANSACTIONS

Electronic devices like smart phones, computer, laptop, tablet, POS machines, ATM etc..., are used to for online means of banking and investments. Most of these devices have become an integral part of an individual's life resulting in online means of banking and investments overtaking the traditional banking methodology. As all of us are aware that Internet also has a negative side which puts all means of online financial transactions at high risk.

Cybercriminals rely on the vulnerabilities present in Internet to seize your hard earned money. Due to this it is a necessity to take extra step to secure your hard earned money and investments. To get an insight to this, let us look at case of common banking fraud where the victim lost money from his bank account without his knowledge. It happened so, that the victim had received a mail from a stranger saying that he won a lottery. To credit the money to his bank account the victim was asked to click on a link where he had to fill his banking details. The victim shared the information on the link thinking that it is genuine. The link was used to divulge information pertaining to the bank account of the victim. With the information received, the cybercriminal could easily withdraw money from his bank account through illegal online transactions. This can happen with anyone of us any time if we are not aware and and take necessary precautions.

Major challenge lies in identifing cyber-attack, when it happens. In the present scenario wherein the life of an individual, technology plays a vital role, it is better to be aware of aspects like how to detect, how to protect and how to recover from cyber threats in financial sector?

With increase in online scams most of us are flooded with lot of questions in his mind like is my money safe online? What are the cyber security threats that can affect the savings of an individual transacted digitally in financial institutions? How can I assure safety to my investment?

Keeping all this in mind, there is a need to learn about cyber issues present in the cyber world to protect yourself and your money.

HOW FINANCIAL FRAUDS HAPPEN ?

Cyber criminals employ various methods to attain the sensitive personal information to execute fraud. Few methods used by cyber criminals are Phishing, Smishing, Vishing, Skimming, SIM Swapping fraud, Fraudulent policy applications, Payment hijacking, Malware, DDos attack, Man in the middle Attack, Ransomware, Business email Compormise.

IMPACT OF ONLINE FINANCIAL FRAUD ON AN INDIVIDUAL

The first thing that comes to mind when we talk about 'impact of online financial fraud on an individual' is the direct financial loss. Victims often pass through wide range of emotional and psychological impacts of fraud. Many panick, and feel angry, freightened, anxious, ashamed and blame themselves after they are cheated. They even feel vulnerable, lonely, violated and depressed and in the most extreme cases, suicidal, as a result of the fraud they experienced.

These emotional and psychological impacts relate to both the stress of financial loss and also the loss of self-confidence that followed the fraud. The experience also may affect relationships with others, making it difficult for victims to trust others. It can be summerised as

- becoming a financial fraud victim carries emotional as well as financial costs;
- Financial and emotional costs vary across fraud categories; and
- Individual personality traits influence the victims' perceptions of impact.

Dos

- ✓ Always keep your device updated, locked & protected with a strong password.
- ✓ Beware of unsolicited calls, texts or emails asking for sensitive financial information.
- ✓ Download applications on your devices from authentic apps stores with good reviews only.
- ✓ Ensure authenticity of applications by validating from links on bank websites.
- ✓ Always verify and install authentic e-wallet Apps
- ✓ Ensure your phone number is protected with a PIN.
- ✓ Make sure the beneficiary's mobile number is correct before transactions
- ✓ Use only verified and trusted browsers & HTTPS secured websites for payments.
- ✓ Ensure you change passwords frequently and promptly if compromised.
- ✓ Ensure that you securely dispose of receipts and statements.

Donts

- × Refrain from clicking suspicious links received in SMS or email.
- × Steer clear of using jailbroken or rooted devices for mobile banking.
- × Never handover your device to strangers.
- × Avoid using a common password for all wallets.
- × Refrain from opening wi-fi or unverified services for making payments.
- × Do not scan untrusted QR codes.
- × Avoid transacting through public devices and on unsecure/open networks.
- × Never allow merchants to store your card information.
- × Do not leave your credit or debit card with anyone.
- × Never share or write down your UPI M-PIN.
- × Refrain from transferring money without verifying the recipient first.
- × Never allow merchants to store your biometrics and card details.
- × Avoid giving away your Aadhaar and personal details