

# Account Takeover & Information Security Awareness



Information Security: To mitigate security risk through outreach, awareness, assessment, policy, and best practices.

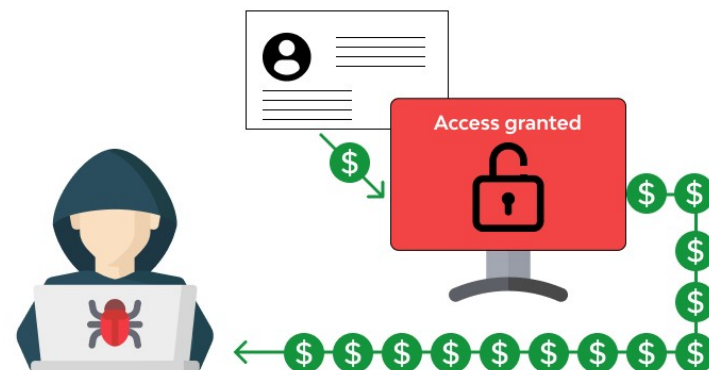
# Introduction

- ▶ Welcome to the Community First Bank educational presentation on account takeover
- ▶ This presentation will help you understand what account takeover is, how it happens, and most importantly, how you can protect your bank account from it



# What is Account Takeover (ATO)?

- ▶ ATO is a type of fraud where a cybercriminal gains unauthorized access to your bank account
- ▶ Common methods used by fraudsters to gain access to accounts include:
  - Phishing scams
  - Malware
  - Social Engineering tactics



# Common ATO Methods

## ▶ Phishing scams

- An attacker sends an email or text message posing as a legitimate entity and requests the user to provide sensitive information or click on a link to a malicious website

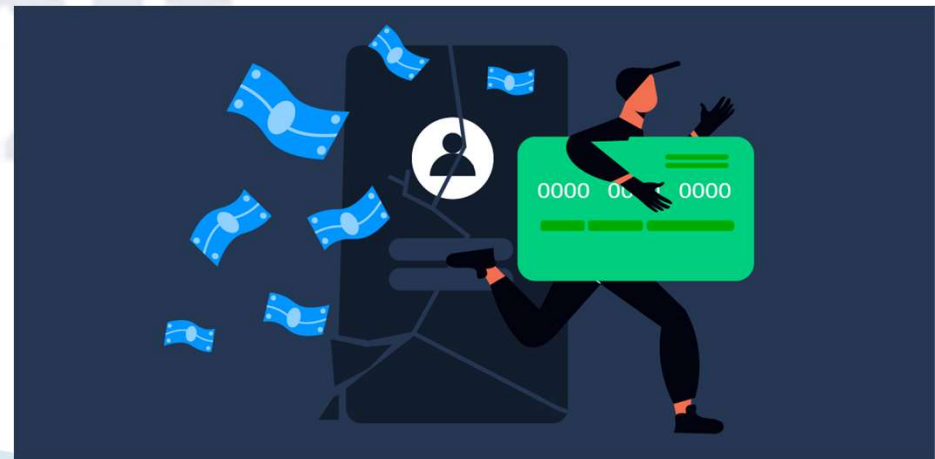
## ▶ Malware

- An attacker can infect a user's device with malware through email attachments or infected websites, allowing them to monitor user activity and steal login credentials



# Common ATO Methods

- ▶ Social engineering tactics
  - An attacker can trick a user into providing sensitive information by posing as a bank representative or use other manipulation techniques
- ▶ Examples of how ATO occurs
  - An attacker gains access to your bank account and makes unauthorized transactions, changes your account details, or transfers funds to another account



# The Impact of Account Takeover

- ▶ The financial and non-financial impacts of account takeover can be severe and long-lasting
- ▶ Financial impacts
  - Loss of funds, overdraft fees, and potential damage to credit score
- ▶ Non-financial impacts
  - Stress, time-consuming recovery efforts, and potential damage to reputation



# Best Practices for Preventing ATO

- ▶ Use strong and unique passwords
  - Use a different password for each account and avoid using easily guessable information like your name, birthdate, or common words
- ▶ Enable two-factor authentication (2FA)
  - 2FA adds an extra layer of security to your login process by requiring an additional code sent to your phone or email, a biometric factor like a fingerprint or facial recognition, or a security key



# Best Practices for Preventing ATO

- ▶ Monitor account activity regularly
  - Regularly review your account activity and report any suspicious transactions to customer service
- ▶ Keep your software up to date
  - Update your computer, smartphone, and other devices regularly with the latest security patches and updates to avoid known vulnerabilities
- ▶ Be cautious of unsolicited emails or phone calls
  - Be wary of emails or phone calls requesting your personal or financial information and never provide sensitive information unless you have verified the legitimacy of the request



# How to Identify if your Account has been Taken Over

- ▶ Unexpected withdrawals or transfers
  - Look for unusual transactions or activity in your account, including transfers to unknown accounts or withdrawals you didn't make
- ▶ Changes in account information
  - Keep an eye on any unauthorized changes to your account details such as email addresses, phone numbers, or account passwords
- ▶ Notifications of new devices or IP addresses
  - If you receive any such notification and did not authorize the access, contact customer service immediately



# What to Do if your Account is Compromised

- ▶ Contact customer service immediately
  - Report any unauthorized activity to the Fraud department
- ▶ Change your passwords and enable two-factor authentication
  - Reset all your login credentials and enable 2FA to ensure that any attacker is locked out of your account
- ▶ Report any unauthorized transactions
  - If you see any unauthorized transactions in your account, report them to the Fraud department immediately



# Conclusion

- ▶ ATO is a serious threat that can result in financial and non-financial losses
- ▶ By following best practices like using strong passwords, enabling 2FA, and monitoring your account activity regularly, you can significantly reduce your risk of becoming a victim of ATO
- ▶ It's also important to be aware of the warning signs of ATO and know what steps to take if you suspect your account has been compromised.