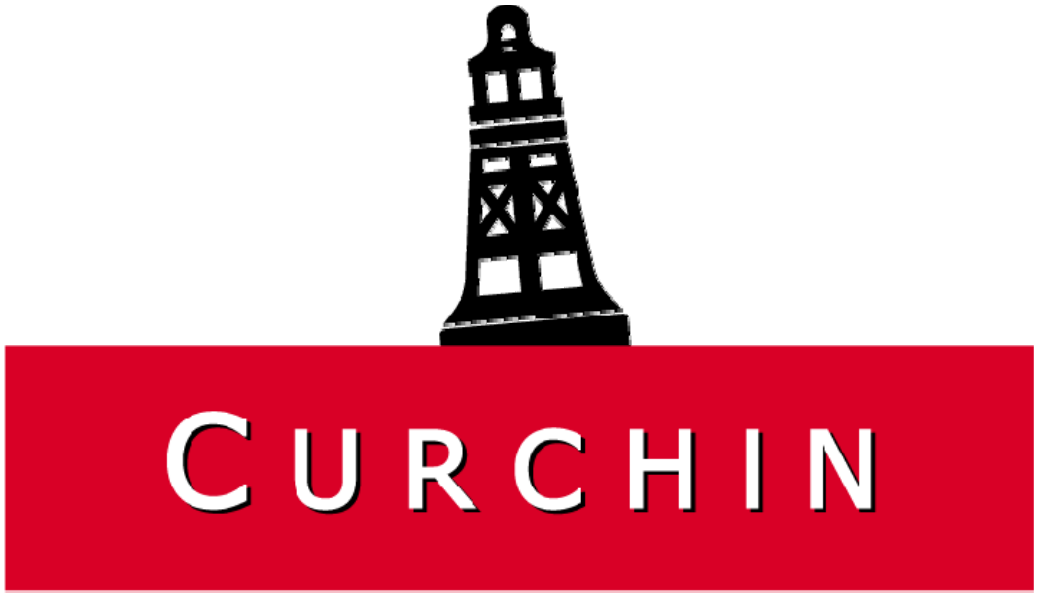


LONG-TERM RELATIONSHIPS ARE ALL ABOUT DEDICATION

Fraud Trends in the Credit Union Industry

NACUSAC CONFERENCE AND EXPO

2017

"You know, you can do this just as easily online."

Headlines

- Missouri Credit Union – exposes information on 39,000 members via its website.

- More than 700 members notified of fraud after skimming device found at Founders FCU– May 2017

- Hudson Heritage FCU – victimized by auto loan fraud ring - $135,000

- Langley FCU - $167,000 - auto loan fraud.

- Target Breach – hit credit unions for 30.6 million

- 10,000 twitter accounts belonging to Department of Defense employees targeted by Russians

Significant Trends

- More identity theft victims, but less money stolen
  - Estimated that $35,600 stolen per minute via identify theft
- EMV – has caused new account fraud to double
- Consumer choices negatively impact fraud detection
  - Consumers who do not trust their financial institutions less likely to use transaction monitoring, email alters, etc. Fraudsters use these consumer information 75% longer and have greater fraud loss $$$'s
- Mobile banking fraud on the increase
  - Increasingly become targets for hackers, mobile payment systems- malware attacks


So you're a complete stranger and you want my name, social security number and mother's maiden name? Sure, why not?
SecurityElements.com

Significant Trends

- Social Engineering Fraud on the increase
  - Telephone continues to be the weakest link
- Proliferation of social media increases risk
  - Introduction of malware via social media networks
- Fraudsters organizing on a larger scale and looking to target larger data sets
  - Collaboration among specialists, on-line cyber attack kits for sale.
- Cyber Attacks will target smaller businesses.
  - Rules based detection systems will be replaced by artificial intelligence systems

I THOUGHT THAT CHIP THING WAS SUPPOSED TO STOP FRAUD.

- It is estimated that only 80% of ATM machines in the United States will be EMV compliant by the end of 2017(Europay, Master Card, Visa)
- As of December 2016, only 30% of merchants were EMV compliant

  -Resulting in increased targeting of

  - Noncompliant ATMs retail outlets
  - Restaurants
  - Gas stations
  - Small merchants
  - Card Not Present (internet)

New Account Fraud

- Compromised credentials (survey 332 victims)
  - 77.% directly compromised (loss of wallet, mail, smartphones)
  - 47.4% targeted through hacking, phishing emails, or a breach
- Online account openings account for 26% of all new accounts
  - Greater anonymity
  - Name, Social security #, date of birth
- Elaborate schemes used to open accounts
  - Impersonating professionals, fictitious businesses, etc.

New Account Fraud Continued

- Deposits of fraudulent checks
  - Fraudulent checks account for 75% of all fraudulent payment schemes. 34% debit/credit cards/27% wires
- Fraudulent Loans
- Red Flag Programs
  - Employees not trained
  - Employees quick to overlook discrepancies
  - Use of non-government issued id's

Automated Clearing House (ACH)

- Credit Union's that originate transactions at most risk
- Account take over
  - Customer credentials compromised
  - ACH transactions set up to move funds to another party
  - ACH transactions altered to different recipient
  - Payroll
- Booster Payments
  - Member (fraudster) makes fraudulent on-line payments to credit cards (may be in excess of card limit)
  - Creates a debit transaction to pull funds from an account at another institution
  - Other institution returns the transaction for insufficient funds or no such account.
  - Fraudster spends the credit card balance

Cyber attacks, Malware and Ransomware

- Hackers targeting credit unions, small banks and professional firms
- DDos (Distributed Denial of Service)
  - Multiple systems attack a single target
  - Result is the user's of the target can not use it services
  - Looking for gateways,
  - infect devices communicating with servers
  - Looking to disrupt
- Spear phishing
  - Spoofing –legitimate looking email
  - Malware attached or imbedded in the email
  - Ransomware
    - Encrypts target data,
    - Demands a ransom, usually in bit coin

Social Engineering

How do the bad guys get the information

- Direct Compromise
  - Lost/stolen wallets
  - Phone scams
  - Mail intercept
  - Home computer and emails
- Data Breaches
  - Introducing malware into a retailer's payment systems
  - Introducing malware into a financial institution via emails
- According to Verizon, in 2016, 30% of spear phishing targets are opened by their targets

Social Media as a Way to Get Past Defenses

- As anti-virus software and user awareness of email risks improves, hackers are turning to social media to make their way onto computers.
- Why – we trust social media more, we feel like we are among friends
  - Social media monitored for common interests
    - By monitoring public posts attackers can easily see your favorite sports teams, music group,
  - Tailored message with links put out by robot accounts
    - Vacations,
    - News updates
    - Items of interest
- Department of Defense –
  - Wife of employee clicked on a twitter link, shared the account with DoD employee, infected the employee as well.

"WELL, I *TOLD* YOU NOT TO OPEN THAT ATTACHMENT!"

How do we protect ourselves

- New Accounts
  - Strict adherence to account opening procedures including using official picture ids
  - Use Account Owner Authentication tools (AOA)
    - Instant feed back
    - uses a variety of elements to confirm id, phone #'s, emails, social security numbers, etc.
    - Train employees to focus on discrepancies
  - Flagging new accounts as high risks
  - Limiting or monitoring dollar amount or volume of transactions for a period of time

ACH Transactions

- Require a high levels of user authentication.
  - User names, strong passwords, pins, multiple levels, force password changes.
- Recommend customers reconcile banking transactions every day.
- Limit $ amount of transactions
- Limit credit card payment amounts to balance due
- Require corporate customers
  - to use dedicated machines, that do not have email or web-browsing services
  - Use dual controls to originate ACH or wire transactions
- Monitor account maintenance changes including password changes and resets
- Transaction monitoring software – especially overseas transactions

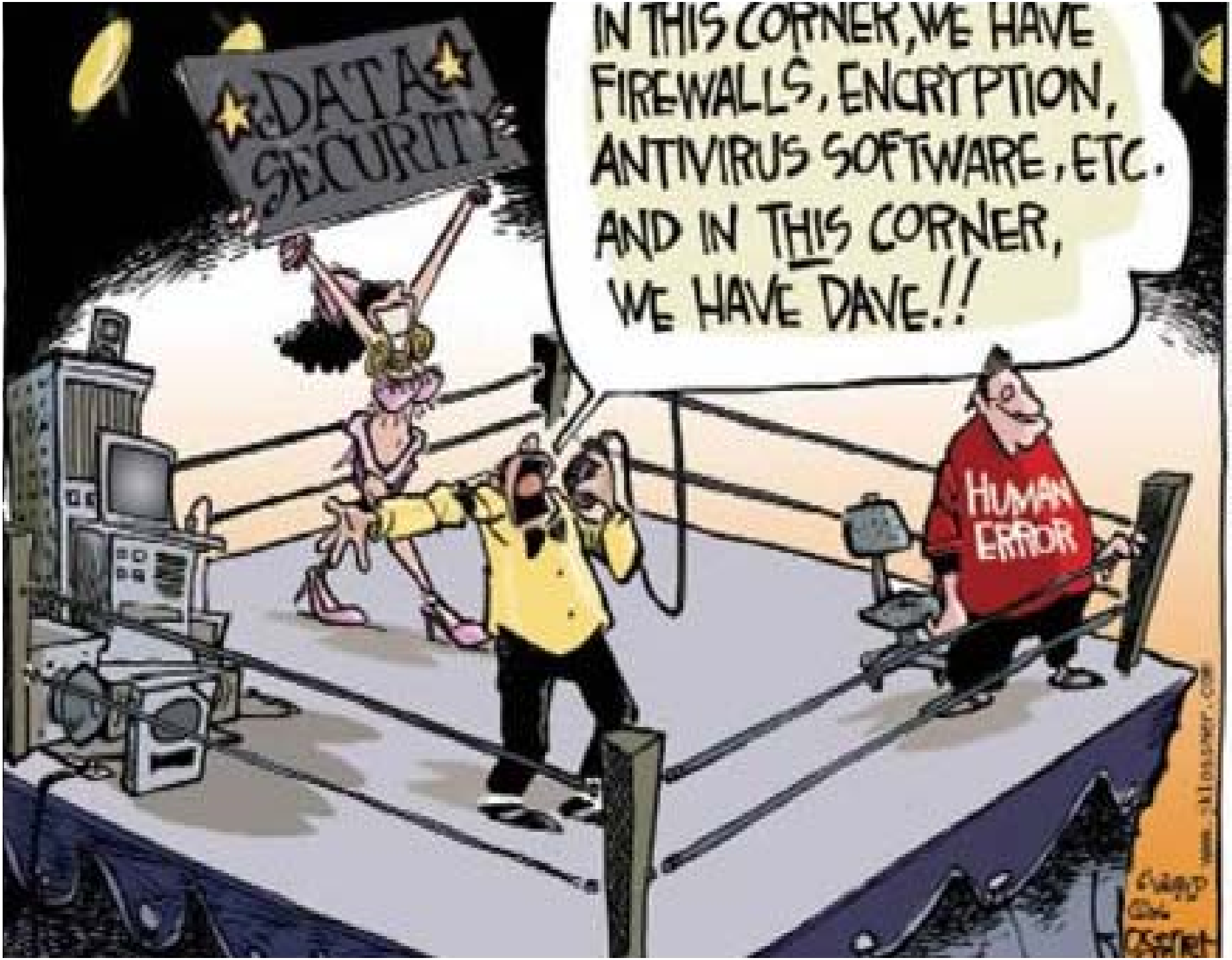
Protecting Against Cyber Attacks

- Educate your members
  - Millennials most likely to be scammed (optimism bias)
  - Customers are unaware of how little information is required to steal an identity.
  - Educate them on how to protect their information
- Educate your employees
  - Establish appropriate procedures and protocols.
  - Emphasize their importance
  - Prohibit use of personal email & social media accounts on credit union computers.

"You've been working awfully hard lately. If you need a little fresh air and sunshine, you can go to www.fresh-air-and-sunshine.com"

Protecting Against Cyber Attacks Continued

- Perform a Cyber Security Risk Assessment
- Do not rely solely on fire walls and penetration tests
  - Typically firewalls are monitored by third parties
  - Can your firewall tell you if you have been attacked or you are under attack
  - Internal monitoring software
- Keep your computers up to date
  - Patches, operating systems, anti-virus/malware detection systems.
- Only permit registered devices to access your system.
- Require members to use multi step authentication when logging in
  - Biometrics, coupled by strong passwords and security questions
- Implement a security awareness program
  - Make it part of your culture



CURCHIN

LONG-TERM RELATIONSHIPS ARE ALL ABOUT DEDICATION

Questions/Discussion