Credit Union Security: What Should You Do?

Learning from Other's Mistakes

Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

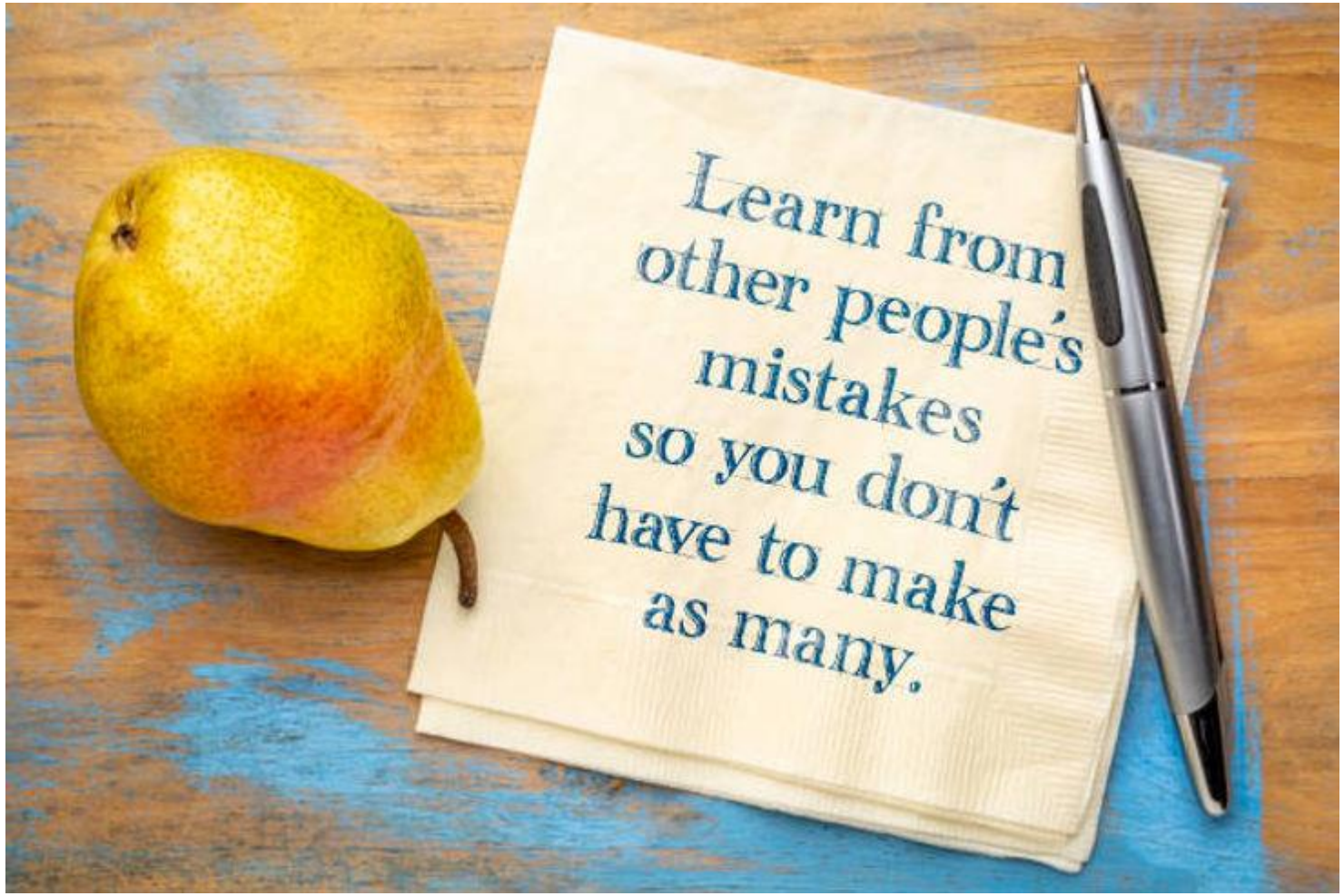
No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

"Credit Union Security: What Should You Do?" discussed in this presentation is the current version with effective date of 2/13/2024.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.

General Overview

- Thoughts on Mistakes
- Stories
- What Went Wrong
- What Was Learned
- Questions



Story #1

You Called Who?

You Called Who?

- Internal Newsletter to all staff with links
- Staff member clicks on link to read more
- Clicks on Google Ad link in the corner of the screen
- Scareware Popup / pleased call this 800 number

You Called Who?

- Attempts to talk to supervisor
- Still had message on the screen, so they called
- Phone call lasted for more then 15 minuets
- Followed instructions and installs software (Any Desk)

Controls

- Second Gen AV / EDR
- No Local Admin rights for staff
- Security Awareness training / updated annually
- Monitoring of outbound web traffic / web filtering

What Went Wrong

- Staff member did not follow training and protocols
- Browser install not identified as a threat
- Failure of imagination?

What Was Learned

- Meeting with EDR vendor to review additional controls
- Blocks added to EDR for Any Desk application
- Security Awareness training updated with this situation
- Web monitoring rules adjusted
- Removed clickable links from internal communication

Questions

Story #2

Infinite Phish Loop

Infinite Phish Loop

- Multiple VFCCU staff receive the same odd message from an Executive at a member CU
- Reported to Info Sec for review / found malicious link meant to compromise the recipients M356 account
- Contact member CU to report the issue and offer help
- Block sender address till issue is resolved / warning sent to internal VFCCU staff

Infinite Phish Loop

- Multiple VFCCU staff receive the same odd message from an Executive at **(another)** member CU
- Reported to Info Sec for review / found malicious link meant to compromise the recipients M356 account
- Contact member CU to report the issue and offer help
- Block sender address till issue is resolved / warning sent to internal VFCCU staff

Infinite Phish Loop

- Multiple VFCCU staff receive the same odd message from an Executive at **(yet another)** member CU
- Reported to Info Sec for review / found malicious link meant to compromise the recipients M356 account
- Contact member CU to report the issue and offer help
- Block sender address till issue is resolved / warning sent to internal VFCCU staff

Controls

- Microsoft M365 email platform
- Active spam filtering and security controls
- Security Awareness training / updated annually
- Quarterly phishing tests to all staff

What Went Wrong

- Assumed something coming from another CU executive was safe
- No MFA/2FA on M365 login
- Poor passphrase hygiene

What Was Learned

- Added MFA to M365 login / set passphrase life to 90 days
- Security Awareness training updated with this situation
- Stronger phishing tests
- Slow down and check for red flags

Questions

Story #3

Gift Card Target

Gift Card Target

- CU Staff member gets an after-hours text message claiming to be from the CEO/CFO/Ops Manager etc
- Story about an employee incentive program
- Asks them to buy $2500 in Target gift cards (CU credit card)
- Scratch the back and send the conformation codes

Gift Card Target

- Following morning things did not “feel” right
- Talked to management at CU and found that no such program was being put in place
- Called VFCCU for assistance
- Contacted Target card support – cards were spent online within moments of the codes being sent

Gift Card Target

- Investigation was opened by Target’s fraud department
- Police report filed with the local and state police in the area of the CU

Controls

- Basic Security Awareness training covering CU policies only (annually)

What Went Wrong

- Staff member assumed the text message was from CEO/CFO/Ops Manger

- Never questioned or confirmed

What Was Learned

- Staff with CU issued mobile devices added contacts
- Security Awareness training expanded to cover this type of attack and others
- All staff trained to “call back” and confirm all requests not made through approved channels

Questions

Story #4

I Approved A Fraud Wire… That I Requested?

I Approved A Fraud Wire…?

- Staff member at a CU receives and email claiming to be from the CEO, asking for a $100,000 wire to be sent out
- Wire is created in the wire system according the instructions in the email
- Wire requires dual control to send out, staff member stops in the CEO's office and asks them to approve it
- Phone call made to VFCCU asking if we can stop / cancel / request a return of the wire

Controls

- Basic Security Awareness training covering CU policies only (annually)
- Quarterly phishing tests on all staff
- External Email Flag
- Dual control on all wires

What Went Wrong

- Assumed something coming from the CEO was OK / never questioned it

- External email flags not be checked by all staff

What Was Learned

- Security Awareness training expanded to cover this type of attack
- All staff trained to question/confirm all wire requests not made in person
- Reenforce all staff training on external email alerts
- Stronger Phishing tests around this type of attack

Questions

Contact Information

- Michael Bechtel
- Information Security Analyst
- mbechtel@vfccu.org
- Toll-Free (800) 622-7494 ext. 1101
- Website: www.vfccu.org/solutions_mobile/risk_management.html