Fiscal Fitness – Technology & Security

AGENDA

- Greeting and welcoming to refreshments
- Introduction
- Discussion of banking and technology trends
- Review of financial and information security concerns
    - Identity Theft
    - Information Security
    - Phishing
    - Phone Fraud
    - Hacking
    - Various Scams
    - Computer Security
    - Card Security
- Review of technology available with Mountain Valley Bank to help keep your finances and information secure as well as provide ease for managing your finances
    - Online Banking
        - MVB Categorize
    - Mobile Banking
    - Tokenization (Digital Wallet)
    - Bill Pay
    - Popmoney
    - Mobile Deposit Capture
    - CardValet®
    - Credit Cards
- Request completion of surveys and direct attendees to breakout stations for help with individual issues or questions
    - Online Banking
        - Bill Pay
        - Popmoney
        - Credit Cards
    - Mobile Banking
        - CardValet®
        - Mobile Deposit Capture
        - Mobile Wallet
- End

Fiscal Fitness – Technology & Security

IDENTITY THEFT

- Read credit card and bank statements carefully and often. With technology and the use of online and mobile features, you can review many of these any time, any place.
- Know your payment due dates to ensure bills show up when you expect them.
- Read health insurance plan statements to ensure the claims paid match the care you received.
- Shred documents with personal and financial information.
- Review each of your credit reports at least once a year.

INFORMATION SECURITY

- Be aware of everywhere your information may be shared or sold. Potential areas might be:
    - Shopping loyalty cards may share location and shopping history
    - Prescription history
    - Coupon apps may share purchase and location history
    - Location information on apps you may use
    - Web traffic and search history (articles read, sites visited, etc.)
    - Social media profile information, quizzes, surveys, etc.

PHISHING

Do's

- Review the email for grammar and spelling
    - Some attacks will have noticeable misspellings and other grammatical errors. Unusual spacing and/or formatting can also be a sign of phishing.
- Inspect the links
    - Attackers embed malicious URLs into seemingly legitimate ones in their emails. Use the mouse to hover over the link to determine if there is an embedded URL.
- Validate the request
    - If you receive an email from a fellow employee or vendor requesting information, pick up the phone and verify the request. Always use contact numbers from external websites – NOT the ones included in the potential phishing email.
- Alert the appropriate personnel
    - If you think you have received a phishing email, get it to the proper person in IT. They can try to block others from receiving it or block access to links that were included in the phishing email. Don't hesitate to forward suspicious emails to the appropriate IT staff!
- Use common sense
    - If a vendor of three years has never asked for your password information through email, they probably wouldn't be starting today. If a coworker of two years has never sent you an attachment and sends you one today and tells you to enable macros, don't. Question requests outside the norm and use common sense when fulfilling requests.

Fiscal Fitness – Technology & Security

Don'ts

- Don't trust the sender
    - It doesn't take time or skill to "spoof" or impersonate the sender of an email. From your boss to the President of the U.S., attackers can assume the identity of anyone.
- Don't be so quick to reply
    - Sometimes attackers are just looking to find valid email addresses within an organization or to identify the naming convention used within an organization. By replying to an email like this, even if it's only to give the would-be attacker a piece of your mind, you only help the attacker determine that the email reached a recipient.
- Don't open that attachment
    - Attachments once thought of as harmless (Word, Excel, PDF) are now used to launch various attacks against end-users. If you're not expecting an attachment, don't open it!
- Don't give out personal information
    - Most companies won't ask you to transmit personal information, account information, or passwords via email. Similar requests should raise suspicions and be reported.
- Don't be embarrassed
    - Don't be embarrassed that you fell for it. Don't try to fix it yourself. Don't assume you'll be in trouble. Alert the appropriate IT personnel or authorities.

PHONE FRAUD

- Usually start with a phone call but can also start with an online ad or piece of mail.
- Steps to prevent:
    - Recognize – Recognize the signs of telemarketing fraud.
        - Callers who ask for money first.
        - Callers who want to know your bank account, credit card, or Social Security number.
        - Scammers may even have your billing information before they call you.
        - Often, they are trying to get you to say ok so they can claim you approved a charge.
    - Report – Report to the Federal Trade Commission.
        - Ftc.gov and click consumer complaint link.
        - The more info on the company and when they called you that you are able provide the better.
    - Register – Register your number on the national Do Not Call registry.
        - Register online at donotcall.gov
        - Be sure to complete the process by clicking the link in the confirmation e-mail you receive
        - Register toll free at 1-888-382-1222 by calling from the number you wish to register

Visit **ftc.gov/phonefraud** to learn more about how to recognize and report telemarketing fraud.

Fiscal Fitness – Technology & Security

HACKING

Hackers use computers to gain unauthorized access to data. This can often be evidenced by friends and family receiving e-mails or messages that you never sent, or you may unable to log-in to your own account. If you fear you have been hacked, follow these helpful measures.

- Update or install security software from a company you can trust and set it to update automatically.
- Scan your computer with this software and delete anything that it identifies as suspicious and restart your computer.
- If you can get into your accounts, change your passwords. Make sure to change your password on any account that used the same or similar password to the account you feel may have been compromised.
- There is software out there that manages passwords if you need help doing so.
- If you can't get into your account, check with your service provider to see how you can restore your access.
- Once you regain access, check your account settings to ensure no one added any links allowing your information to be forwarded to someone else.
- Finally, let family and friends know you were hacked.

MONEY WIRING SCAMS

Dishonest people might convince you to wire money to them. They might say:

- you just won a prize, but you must pay fees to get the prize
- you need to pay for something you just bought online before they send it
- a friend is in trouble and needs your help
- you got a check for too much money and you need to send back the extra

These are not good reasons to wire money. Never wire money to someone you do not know.

Fiscal Fitness – Technology & Security

COMPUTER SECURITY

Ways to foil hackers and protect your financial information:

- Install security software from well-known companies and set it to update automatically.
- Set your operating system and web browser to update automatically. If not sure how, use the help function and search for automatic updates.
- If you get a phone call, email, text, or a pop-up that says you have a virus don't buy the story or the software they're selling as it could be a trick.
- If someone asks for your personal or financial information (Social Security, Credit Card, or Bank Account number) ask why they need it and how they protect it.
- If you think you've found a good deal online, dig deeper. Search the company online with the word review or complaint. Look for the company's physical address and phone number as well.
- Don't provide your personal or financial information unless the website is secure. You can tell if it is a secure website by the "s" in https in the website's url. That "s" stands for secure and means that the information you send is encrypted and protected.
- Make passwords at least 10 characters and a mix of numbers, letters, and special characters. Don't use name, birthdate, or common words.
- Don't use the same password for several accounts because if it is compromised, hackers have access to much more.
- Keep passwords in a secure place and don't share them with anyone.
- Backup your files to ensure you have info safe if something happens to your computer.

CARD SECURITY

- Never reveal sensitive numbers or passwords.
- Let your card issuer know you will be traveling before you go on a trip outside your usual area.
- Don't respond to click links inside suspicious e-mails.
- Monitor your account online daily for suspicious activity.
- Use card controls to turn your card off when not in use and/or monitor it's use.
- Immediately contact the card issuer when unusual activity is observed.

Fiscal Fitness – Technology & Security

ONLINE BANKING

- go to mtnvalleybankonline.com
- Click “Enroll Now” below the username field
- Read through and accept the terms and conditions by clicking “Enroll in Online Banking”
- Complete all the requested information to enroll (Your PIN will be either the last 4 of your Social Security number or your ETHEL PIN if you have used ETHEL)
- Type your desired username and password (password must be between 8-17 characters, contain at least 1 number, and at least 1 letter)
- Fill in and confirm your e-mail address. Then choose and answer 3 security questions
- You now may download the MVB mobile app or enroll in text banking

MOBILE BANKING

- Once signed up for Online Banking, go to your app store on your phone and search for Mountain Valley Bank (You will see our logo)
- Click the icon, then “Install” on the download screen, then “Accept” to download the app
- Click “Open” then log in using your Online Banking User ID and Password
- Answer your online banking security question
- You are now logged in and have access to all the options and features of our mobile banking app (Account Review, Bill Pay, Scheduled Payments, Popmoney, Mobile Deposit, Instant Balance, etc)

POPMONEY

- Sign into your Online Banking Account, click Bill Pay, and navigate to the Payment Center
- Click on the Popmoney tab or select a person/payee already in your “Send Money” list
- First-time users follow an activation process
- If already activated, and adding a new person/payee click “add a company or person”
- Enter the recipient’s info with email, mobile, or account number to send the payment
- Find the new entry in your “Send Money” list and select the Popmoney delivery method
- Select the funding account, amount, and delivered by date
- Click “Send Money” at the bottom of the page
- Review payment details and click “Submit Payments”

Fiscal Fitness – Technology & Security

ONLINE BILL PAY

- Have your paper bill handy and sign into your Online Banking Account
- Navigate to the Payment Center
- Click the “Add A Company or Person” button
- Search for your biller
- If you don’t find your biller, you’ll need to enter their information
- Enter the account number from your bill
- Fill in the address you would mail your payment to
- Give it a nickname that helps you identify the bill
- Select a payee
- Enter the payment amount
- Select the date you want the payee to receive the payment
- Click “Send Money”

MOBILE DEPOSIT CAPTURE

- Sign into your Mobile Banking app and click on Deposit in the apps main menu
- Endorse the back of you’re the check you are wanting to deposit
- In the app select “Deposit Check”, choose the account to deposit to, and enter the amount
- Take a photo of the front of the check against a clear background
- The whole check must be visible, in focus, and well lit
- Repeat the process for the back of the check
- Once images have been captured, review and confirm your deposit
- You can check the status of your deposits at any time
- *Tip: Note on the check “Mobile Deposit” and keep for your records

CARDVALET®

- Download the CardValet® app on your device and select new user
- Enter your 16-digit card number
- Enter additional card details as requested
- Validate your identity in one of three ways (e-mail verification, last 4 or your social, or conduct a PIN transaction)
- Create your user name and password and log in
- Turn your card on or off
- Set control preferences (spend limits, location limits, merchant type limits)
- Set Alert Preferences (Use alerts based off location, merchant types, or amount spent)
- Review transactions