STAY INFORMED.
STAY PROTECTED.
STAY CONFIDENT.

SkyPoint FEDERAL CREDIT UNION

- SkyPoint's tools and services that help protect against fraud.
- **Featured Guest Speaker**:
  Detective Cindy Miranda
  Financial Crimes Section
  Montgomery County
  Police Department
- Guidance on how we support members who have experienced or may be at risk of fraud
- We'd love to hear your questions in our Q&A session.

*Information provided in this presentation, including all materials, should not be construed as legal services, legal advice, or in any way establishing an attorney-client relationship. Information may have changed since this presentation was prepared. This information is intended only to be a summary and is not all inclusive.

SkyPoint Fraud Prevention Tools

Push Notifications & Account Alerts
Real-time notifications for transactions, logins, and balance changes.

Multi-Factor Authentication (MFA)
A second layer of login security beyond your password

Debit Card Controls
Freeze, set limits, and manage your card directly in the app

EMV Chip Technology
Reduces counterfeit card fraud compared to magnetic stripes

Fraud Reporting & Dispute Tools
Quickly flag and dispute unauthorized charges

Transaction Monitoring
Automated systems watch for unusual or suspicious activity 24/7

Regular Statements & Activity Reviews
Review your statements monthly to catch discrepancies early

Internal Safeguards
We actively monitor for unusual activity, provide member education, and work alongside you to help prevent fraud.

Financial Crimes Section
Detective Cindy Miranda
CFCI, CFE

Police Headquarters
100 Edison Park Drive
Gaithersburg, MD
(240) 773-6330

Make a report by calling (301) 279-8000 or visiting your local police district station

Disclaimer

This presentation is an educational tool and while names, photographs, cartoons and other information may be included – it is not meant to cause injury, embarrassment or harm to any individual or entity.

The information is based on the presenters own personal and professional experience.

Information was obtained from cooperating law enforcement agencies, financial institutions, businesses, victims and other numerous sources.

MCPD Financial Crimes Section

The financial crimes section is comprised of:

- 1 Sergeant –
- 4 Sworn Fraud Detectives –
- 1 Civilian investigator
- Handful of interns and volunteers

What we do:

Follow-up Investigations:

- Receive over 400 reports a month
- 4,000 to 5,000 reports a year
- 3-4 reports are assigned to a Detective per month
- Our cases involve: Substantial monetary loss, multiple victims, credit cards, embezzlement, financial exploitation of a vulnerable adult, etc.

Montgomery County Cases 04/01/2025 to the present

Offense	Distinct Count of CR #
FRAUD - IDENTITY THEFT	1093
FRAUD - ILLEGAL USE CREDIT CARDS	688
FRAUD - CONFIDENCE GAME	510
FRAUD (DESCRIBE OFFENSE)	404
FORGERY OF CHECKS	251
FRAUD - SWINDLE	87
EMBEZZLE (DESCRIBE OFFENSE)	87
FRAUD - IMPERSONATION	68
FRAUD BY WIRE	48
FRAUD - HACKING/COMPUTER INVASION	45
FORGERY (DESCRIBE OFFENSE)	44
FORGERY - PASS FORGED	24
FRAUD - FAILURE TO PAY	24
FORGERY OF OTHER	22
BAD CHECK – INSUFFICIENT FUNDS	17
FRAUD - MAIL	16
COUNTERFEITING - PASS COUNTERFEITED	12
COUNTERFEITING (DESCRIBE OFFENSE)	12
EMBEZZLE - BANKING-TYPE INST	10
COUNTERFEITING	10
EMBEZZLE - BUSINESS PROP	7
FRAUD - FALSE STATEMENT	6
FRAUD AND ABUSE - COMPUTER	2
COUNTERFEITING - POSS COUNTERFEITED	2
EXTORT - THREAT INJURE REPUTATION	2
FORGERY - POSSESS FORGED	2
EMBEZZLE - INTERSTATE SHIPMENT	1
FORGERY/COUNTERFEITING - POSSESS TOOLS FOR	1
Grand Total	3455

Current Fraud Trends

Elder Fraud / Exploitation

- Family , Healthcare provider, Home Repair, Telephone / Internet scams, Account Take Over

Phone scams/requesting money

- Romance scams, computer virus (Microsoft pop up), courier pick up scams , lottery scams, government imposter scams, "Pig Butchering" scams, distress scams

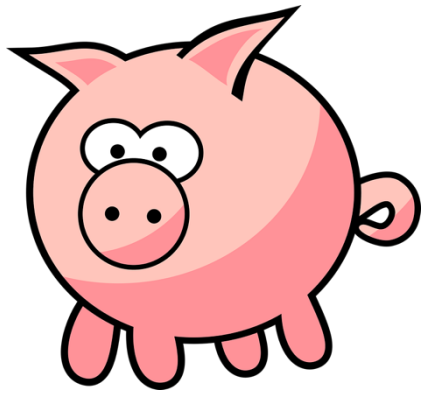
Pig Butchering

What is it?

- "Pig butchering" refers to a type of online investment scam where criminals build trust with victims, often through romance or fake investment opportunities, before luring them into fraudulent schemes to steal their money.

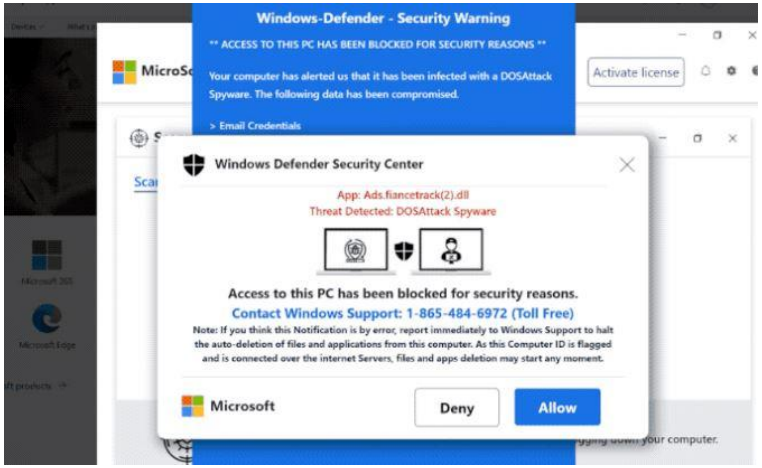
How?

- Download an APP on their phone
- Monitor the investments going up (this if fake)
- Make the victim pay more money to withdrawal the “investment”
- “Investments” are made through Cryptocurrency



Phishing

Microsoft Pop Up Scams



- Message appears
- Victim contacts number
- Allows suspect to gain access
- Another person calls & tells victim she/he needs to secure funds (imposter scam)

How not to become a victim of Phishing

- Do not reply to unsolicited or pop-up information which request "personal identifying information."
- Find a legitimate number to call to verify (do not use the number to call on the screen)
- If you receive a Pop Up on your computer, turn off your computer by doing a "hard shut down"

Government imposter scams aren't new

IRS

RECRUITING

SHERIFF

MONTGOMERY COUNTY

POLICE OFFICER

DEPARTMENT OF POLICE

SCAM

Taxes are overdu
& you need to pay
via gift cards

nstated & you've
been called up for
service

There's a warrant for your arrest & you must pay to have it recalled

Government imposter scams just evolve

A current trend involves couriers picking up gold bullion and other precious metals, gold coins, and US currency (bulk cash)

The typical sequence of events:

1. Notification
2. Initial contact
3. Secondary Contact
4. Secrecy
5. The Realization
   - the scammer “agent” disappears
   - the victim realizes they’ve been scammed
   - the victim faces financial consequences, emotional and psychological trauma, and potential re-victimization

Credit Card Data Breach

- What is a data breach? Intentional or unintentional release of secure information to an untrusted entity.
- Some examples include Target, Kmart, Home Depot, Harbor Freight, etc.

What happens with your info?

- Sold in the dark market (dark web)
- Buyers then use your info to open up credit cards, steal IRS return money, open up bank accounts to commit fraud

How you can protect yourself.....

Don’t open emails or links from people you don’t know

Review your credit report annually

Report lost checks, credit/ATM cards and/or suspicious activity on your bank account immediately

Check your credit card charges and bank account frequently

Do not let someone rush you into making quick money decisions

If you don’t understand cryptocurrency, then don’t use it

Debit Card Scam
"Crackin' Cards"

"Crackin Cards" is a fraud scheme with origins tied to Chicago street gangs

Money mules are recruited through social media applications like Instagram and Snapchat

Mules are typically young adults (18-25yr olds), males & females, all demographics, with bank accounts

Card Cracking

CARD CRACKING

Responding to an online solicitation for 'easy money' and providing a debit card for withdrawal of fake check deposits

A TYPICAL CARD CRACKING SCENARIO

1. A fraudster sends you a social media message to "make quick cash"

IF U WANT 2 MAKE REAL LEGIT MONEY NO SCAM IF U HAVE A BANK ACCOUNT HMU

2. Enticed by the promise of money, **YOU** provide the scammer a debit card, PIN or online credentials—giving them direct access to account

1234 5678 9012 3456

PIN

3. The fraudster deposits a fake check in your account

4. Money is withdrawn immediately at an ATM

5. The fraudster gives the account holder a kickback

6. **YOU** call the bank to report a lost or stolen card, or compromised credentials

7. Bank reimburses the stolen funds to **YOU**

8. **YOU** are now a **CRIMINAL ACCOMPLICE**

[redacted] Following ...

All Tds

Credit unions

All Navy's 

All Boa's

All Chase's

All Well's

[redacted] · Following ...

Pnc🧡

Td💚

Oa❤️

Wells❤️

Regions💚

Chase💙

BB&T❤️

Suntrust🧡

[redacted] ... 🔇 ✕

SWING ME ALL 🏦'S

USAA

WELLS

M&T

NAVY

CHASE

PNC

TRUIST

DISCOVERS

More easy protections

- **Do not give out financial information** (account numbers, credit card numbers or your Social Security number) unless you know the organization or person requesting this information.
- **Notify your bank or credit card company** of any suspicious phone inquiries asking for account information.

Prevention

Solicitations:

If you did not initiate the contact no matter who the contacting individual says they represent, do not react to the solicitation through the channels the solicitor set up.

Urgency:

Think before you withdrawal cash, buy cryptocurrency or wire large amounts of money. Do not let the scammers urgent request allow you to become a victim. Contact a friend/police department/family member first!

WARNING SIGNS THAT YOU MAY BE A VICTIM

Failure to receive bills, statements or cyclically arriving financial information

Denial of credit or vendors who question your credit worthiness

Receive credit cards, checks or any other financial instrument that you did not apply for

Unusual solicitations from vendors outside of your normal pattern

WARNING SIGNS THAT YOU MAY BE A VICTIM

- Failure to receive tax refunds or you receive an audit or tax bill that is unfamiliar to you
- Unfamiliar bills, invoices, lack of receiving your tax return, ACH debits mortgage or rental statements
- Bill collectors start calling/write referencing debt you did not accumulate
- Pinging (1 or 2 dollar charges on your statement often to charities)

FRAUD ALERT

Three Credit Bureaus:

Equifax
Transunion
Experian

Different requirements for the bureaus
There are alerts, temporary freezes and a long-term freezes for victims of identity theft

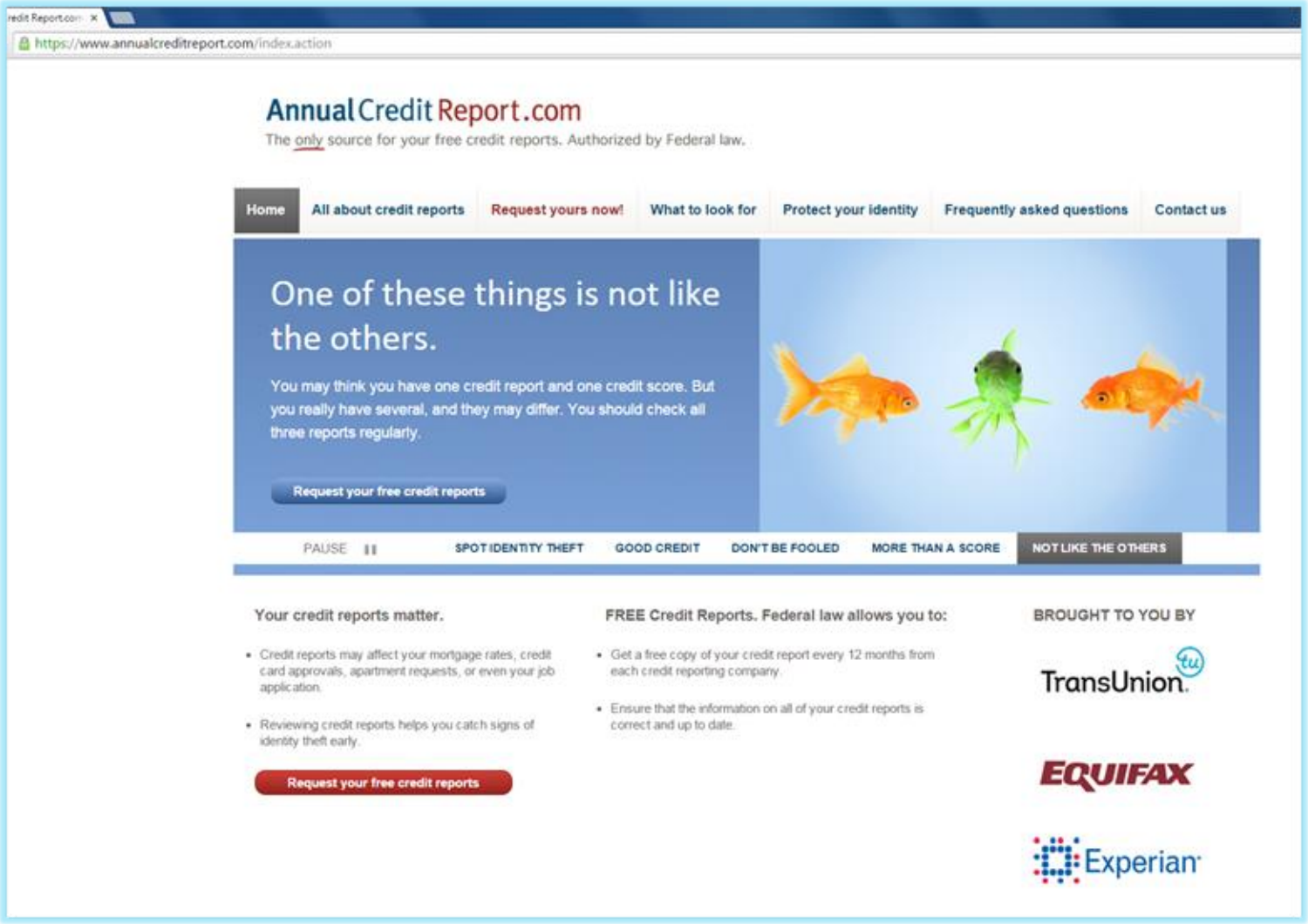
IF YOU ARE A VICTIM

- Make a police report by calling 301-279-8000 or going to your local district police station
- Immediately notify affected creditors, vendors and close all fraudulent accounts
- Get a copy of your credit bureau reports and dispute all unauthorized or unknown transactions
- Request a copy of any fraudulent records created by the imposter, you will need to provide the business with an FTC identity theft affidavit or another acceptable affidavit and your Identity Theft Report (police report).
- File an ID theft complaint with FTC

Free Credit Report/Monitoring

- Make sure you apply for your free annual credit report at annualcreditreport.com, call 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Take advantage of free credit monitoring from companies that have been breached

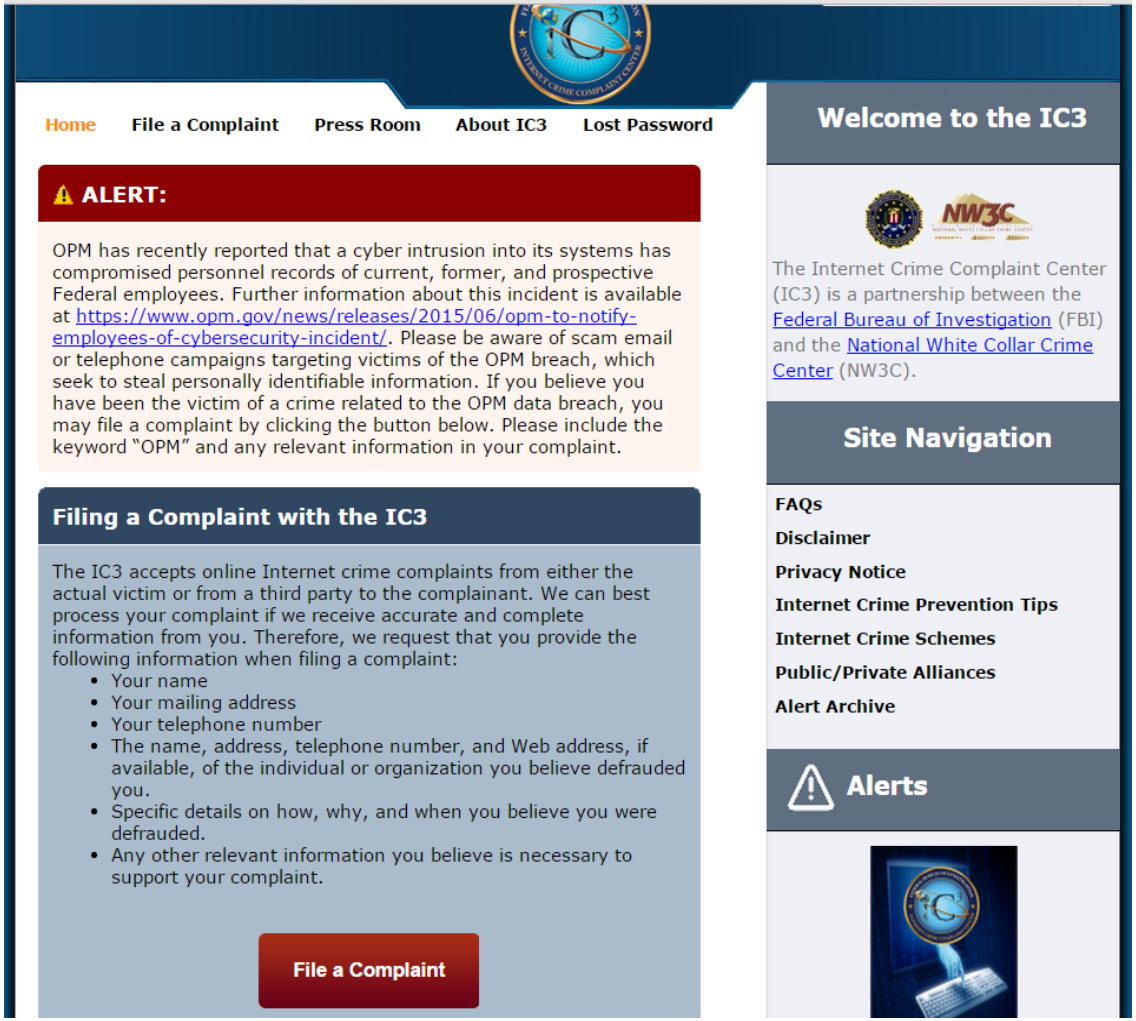

https://www.annualcreditreport.com/index.action
AnnualCreditReport.com
The only source for your free credit reports. Authorized by Federal law.
Home
All about credit reports
Request yours now!
What to look for
Protect your identity
Frequently asked questions
Contact us
One of these things is not like the others.
You may think you have one credit report and one credit score. But you really have several, and they may differ. You should check all three reports regularly.
Request your free credit reports
PAUSE
SPOT IDENTITY THEFT
GOOD CREDIT
DON'T BE FOOLED
MORE THAN A SCORE
NOT LIKE THE OTHERS
Your credit reports matter.
Credit reports may affect your mortgage rates, credit card approvals, apartment requests, or even your job application.
Reviewing credit reports helps you catch signs of identity theft early.
Request your free credit reports
FREE Credit Reports. Federal law allows you to:
Get a free copy of your credit report every 12 months from each credit reporting company.
Ensure that the information on all of your credit reports is correct and up to date.
BROUGHT TO YOU BY
TransUnion
EQUIFAX
Experian

MONITORING

- Early detection significantly reduces the damage and time spent on resolving issues
- Closely review each statement to make sure they accurately reflect all legitimate charges.
- Review your credit report at least once a year preferably twice a year. Look for accounts and inquiries of any kind that seem strange or do not belong to you.
- Check your bank accounts daily

Computer Prevention

- If you have been a victim of an internet scam or fraud please report the crime to the
- Internet Crime Complaint Center (IC3) | Home or (www.ic3.gov).



Do Not Get Depressed

- After listening to this presentation it may seem hopeless at times when dealing with scammers and con-artists. Rest assured the system has greatly improved with servicing victims needs in a timely manner. As always making yourself a less desirable target than others will go a long way to keeping you and your identity safe.

Resources……know who to call

Equifax:
1-800-525-6285 or www.equifax.com
Experian:
1-888-397-3742 or www.experian.com
Trans Union:
1-800-680-7289 or www.transunion.com
Federal Trade Commission (FTC)
1-877-438-4338 or www.ftc.gov
Social Security Administration
1-800-772-1213
Internet Fraud Complaint Center (IFCC)
www.ifccfbi.gov
Annual Credit Report
https://www.annualcreditreport.com/index.action

Any Questions?
Montgomery County Police Financial Crimes
240-773-6330

Protecting Yourself From Fraud

Fraud is on the rise nationwide, with scammers using increasingly sophisticated tactics to steal information, making it more important than ever to recognize warning signs as your strongest line of defense.

SkyPoint
FEDERAL CREDIT UNION

- Unexpected calls, texts, or emails
  Pressure to act immediately
- Requests for unusual payments such as gift cards, cryptocurrency, wire transfers and too-good-to-be-true offers
- Requests for personal or account information
- Romance scams and emotional manipulation

We Are Here to Help Our Members

SkyPoint FEDERAL CREDIT UNION

What Your Credit Union Will NEVER Do

- ✓ Send a text message asking for your personal or account information
- ✓ Email you requesting your debit or credit card details
- ✓ Call you to ask for your PIN or online banking password
- ✓ Ask you to read back a one-time passcode (MFA)
- ✓ Visit your home to verify your account information

What NOT to Do When Someone Contacts You

- ✓ Do not share personal information
- ✓ Do not give account numbers, balances, or card numbers
- ✓ Do not reveal your PIN
- ✓ Do not share online banking credentials
- ✓ Do not provide MFA codes
- ✓ Do not click suspicious links or open unexpected attachments

When in Doubt, Hang Up and Call Us

- ✓ Stop the conversation if something feels off
- ✓ Contact your credit union using the number on your card or website
- ✓ Do not use numbers provided in suspicious messages

Protect Your Accounts

Online Banking

- ✓ Use strong, unique passwords
- ✓ Enable multi-factor authentication (MFA)
- ✓ Only use secure networks
- ✓ Do not click on suspicious links or open unexpected attachments
- ✓ Log out after each session
- ✓ Monitor your account regularly
- ✓ Do not share online banking credentials

Debit Card Safety

- ✓ Protect your PIN
- ✓ Check ATMs and card readers for skimmers
- ✓ Use card controls in the app
- ✓ Report lost or stolen cards immediately
- ✓ Keep receipts and review statements
- ✓ Avoid unnecessary card sharing

Helpful Tips

- ✓ Keep your phone and banking apps updated
- ✓ Install apps only from official app stores
- ✓ Lock your phone with a PIN, password, or biometrics
- ✓ Change passwords regularly

Thank You for Joining!

Any Questions?