



# Identity Theft and Fraud Prevention

## BEST PRACTICES





# Agenda

- Identity theft risks
- Latest cybercrimes and safety checks
- How to detect and avoid scams that can wreak havoc on your finances, credit history, and reputation
- What to do if you become a victim

For informational and educational purposes only.

# Identity theft risk



# How identity theft occurs

- Stolen, lost, or discarded property
  - Documents, computers, wallet/purse, payment card skimming, eavesdropping, shoulder surfing
- Phishing, Vishing, Smishing
  - Emails, phone calls, text messages
- Malicious computer software
  - Viruses, spyware, banking trojans, key-loggers, malware
- Social media sites
  - Facebook, Twitter – putting too much information about you out on the web
- Corporate or organizational databases compromised
- Stolen payment card information
  - ATM skimming

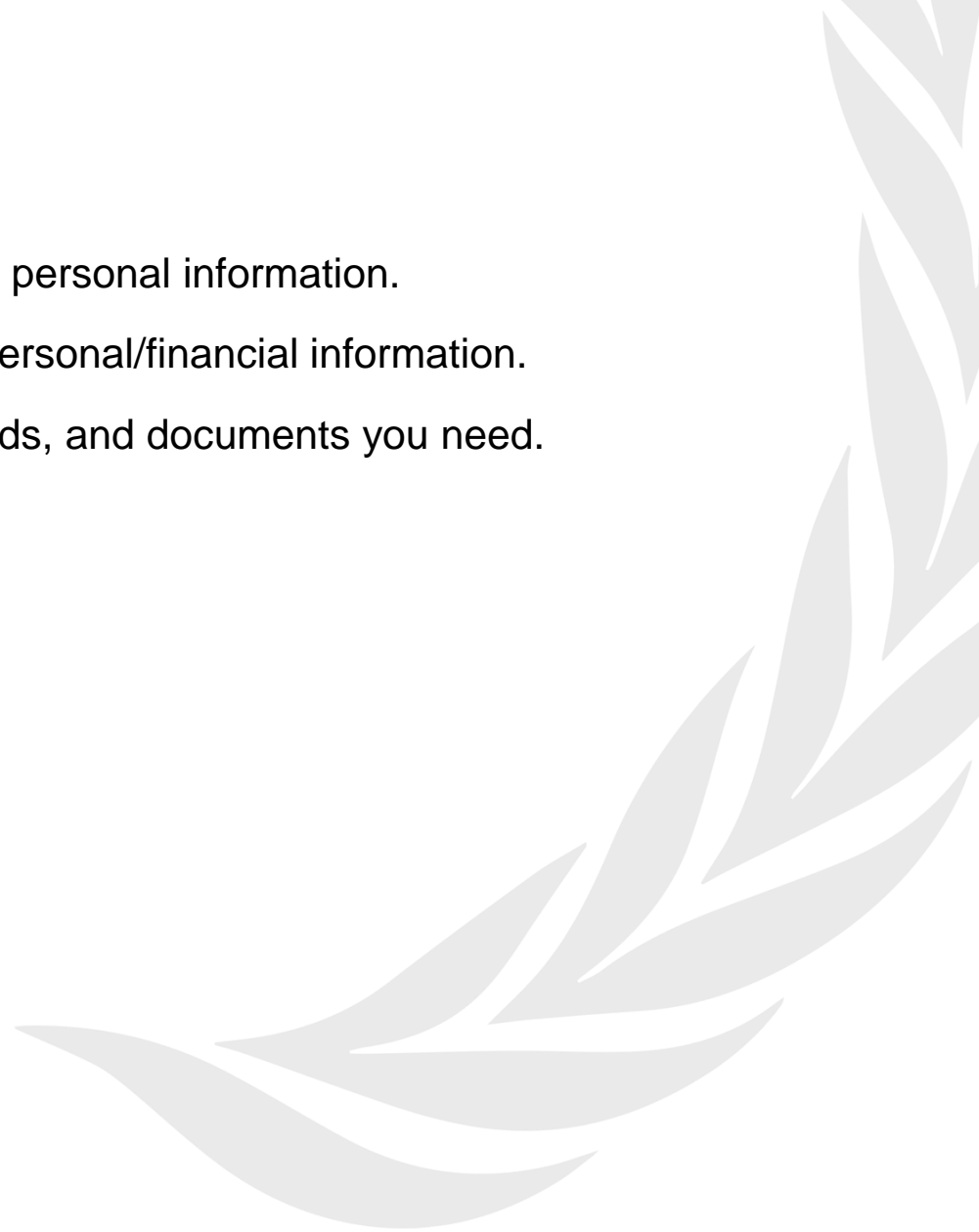
# Minimizing your exposure





# Protect your information

- Protect all documents which contain your personal information.
- Shred unwanted documents containing personal/financial information.
- Carry only the identification, payment cards, and documents you need.



# Phishing emails

- Legitimate organizations will never request personal or financial information through email.
- Never respond to emails asking for your card number even if it appears to come from a trusted source.



# Personal computer

- Ensure your computer's operating system and web browser have the most recent updates.
- Install anti-virus software and keep it updated.





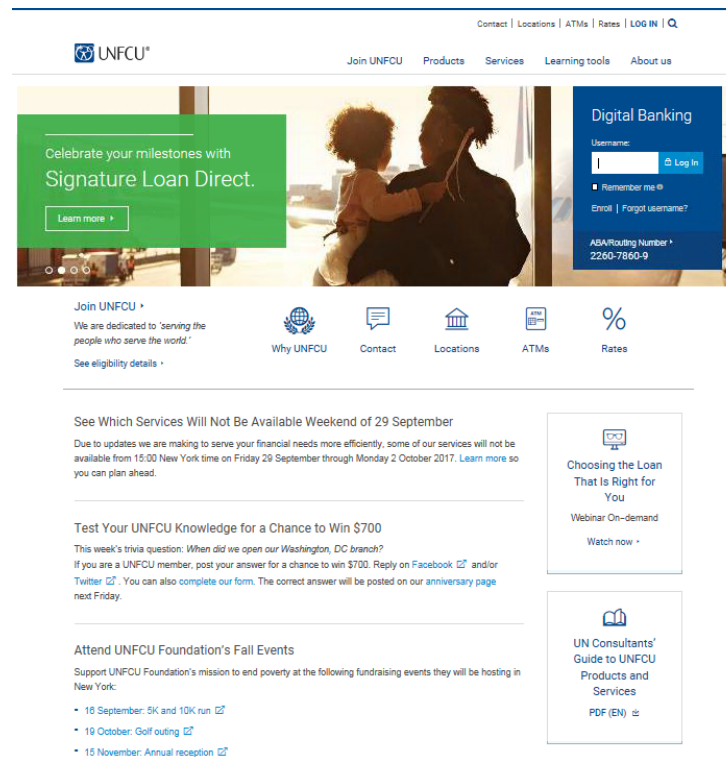
# Passwords

- Choose strong passwords.
- Protect your passwords.
- Use different passwords for different websites.
- Do not share your passwords.
- Change passwords often.
- Consider password managers.



# Online banking

- Use only trusted computers when accessing online banking.
- Never use public or shared computers, such as internet cafés or hotel computers, or public Wi-Fi hotspots when logging into any sensitive website.



# Email

- Never send sensitive information through email.
- Use UNFCU Secure Email service.



# Social media

- Use care in what personal information you post online.
- Enable privacy and security settings.



# ATM skimming

- Skimming is an electronic method used by identity thieves to capture card data.
- A skimmer is a small device that scans the card and stores the information contained on the magnetic stripe
- The information is then used to produce a counterfeit card used by the thief.



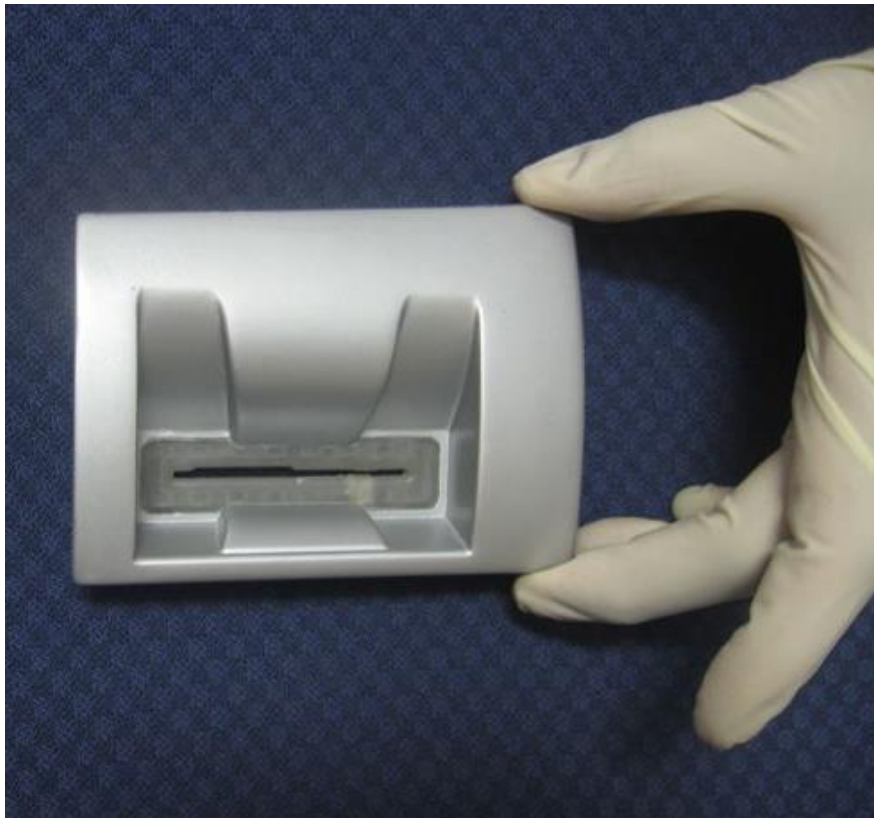
# A typical ATM reader





# Skimming

- Skimmer is a completely self contained unit with its own power supply, computer board, memory card, and video camera.



**Pin Hole Camera facing keypad**



# Skimmer installed over existing ATM reader





# What looks like a safe ATM...



# Today's scams





# US Internal Revenue Scams

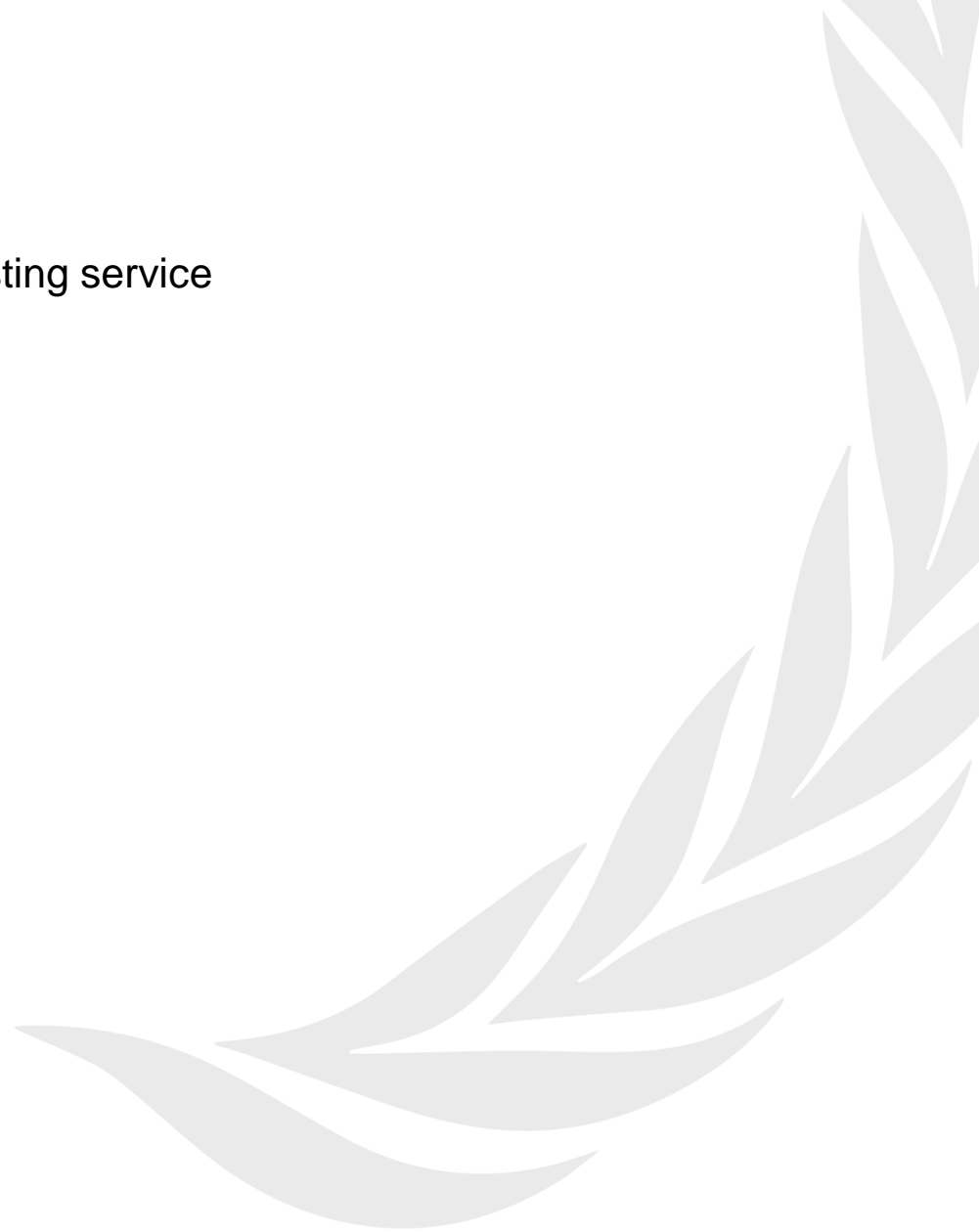
- Email and phishing schemes
- IRS-impersonation telephone scams
- Tax refund scams





# Fake Check Scams

- Selling/renting items through an online listing service
- Work from home schemes
- Sweepstakes/Lotteries





# Computer tech support scams


- Pop-up warning appears on your computer advising of a computer virus and phone number
- “Representative” requests remote access to your computer
- “Representative” advises that a virus was found and to have it removed you must provide your checking account number or credit card

# How to detect and avoid losses



# Monitor your financial account activity

- Review your printed account statements.
- Use Digital Banking to review your accounts and eStatements.

**UNFCU**

**STATEMENT OF ACCOUNT**

SEND INQUIRIES TO:  
UNITED NATIONS FEDERAL CREDIT UNION  
620 SECOND AVENUE, 12TH FLOOR - NEW YORK, NY 10017-4504 USA  
T: (212) 338 - 8100 F: (212) 682 - 5589 - email@unfcu.com http://www.unfcu.org

ANY MEMBER ①  
123 ANY STREET  
ANY TOWN, PROVINCE  
COUNTRY, POSTAL CODE 123

MEMBER NO.	ENDING DATE	BRANCH	PAGE	
000XXX	00-00-00	1	1	XX 01234560000 12345 0

NOTICE: PLEASE SEE REVERSE SIDE FOR IMPORTANT INFORMATION

DATE ②	TRANSACTION DESCRIPTION ④	AMOUNT	FINANCE CHARGE	BALANCE
--------	---------------------------	--------	----------------	---------

# Online shopping

- Only use known and trusted online merchants.
- Most internet browsers will display an icon that looks like a locked padlock when you are on a secure website.
- Only provide sensitive information, such as credit card #'s, over encrypted websites.

✓ *https://*





# UNFCU Visa® EMV payment cards

- Chip and PIN technology for optimized security on UNFCU credit and debit cards
- UNFCU was the first financial institution in the United States to offer a chip and PIN credit card.
- We continue to play a lead advocacy role for smart card technology in the financial services industry.
- Payment cards compatible with Apple Pay, Samsung Pay and Android Pay for mobile payments



# Protect your account information

- Set up Real-Time Fraud Alerts on UNFCU credit/debit cards
  - Free service, easy enrollment
  - You receive a text message to your US mobile device when a suspicious transaction is identified.
  - You reply to confirm whether or not you recognize the transaction(s).
  - Register via [www.unfcu.org](http://www.unfcu.org)
- For US residents, review your credit report. Each of the three major credit reporting agencies is required to provide at your request a free copy of your credit report once every 12 months.
- Visit [www.annualcreditreport.com](http://www.annualcreditreport.com).



# Protection systems - PrivacyMaxx

- Offers advanced and affordable identity theft monitoring and protection for US members
- ID theft restoration
- Internet monitoring
- Lost wallet service
- \$25,000 ID theft insurance
- Free credit report reminder service
- Visit our website for more information, **[www.unfcu.org](http://www.unfcu.org)**

# What to do if you become a victim



# I am a victim. What do I do?

- Report any unusual or unauthorized account activity to UNFCU or other financial institution immediately.
- File a report with your local police where the identity theft took place.
- For U.S. residents, contact the fraud departments at one of the consumer reporting agencies to place a fraud alert on your credit report:
  - Equifax: 1 800-525-6285
  - Experian: 1 888-EXPERIAN (1 888-397-3742)
  - TransUnion: 1 800-680-7289

# Contact UNFCU

- Telephone/Call Center: + 347-686-6000; Toll-free US/Canada: +1 800-891-2471, other international numbers listed on [www.unfcu.org](http://www.unfcu.org). Tie-line +1 212-963-8747
- Email: [email@unfcu.com](mailto:email@unfcu.com)
- Website: [unfcu.org](http://unfcu.org)
- Skype: [unfcu.skype](https://www.skype.com/name/unfcu.skype)
- WebChat
- Secure Email service
- NY branches – UN General Assembly Building, 1B; 2 UN Plaza, 3<sup>rd</sup> floor
- Washington, DC branch – 1775 Pennsylvania Avenue
- Representative Offices in Entebbe, Geneva, Nairobi, Rome, and Vienna

# Your financial safety is a top priority at UNFCU

- By following basic security guidelines, you can surf the web, conduct your financial transactions or shop for your favorite items, while helping to prevent the likelihood of your personal information being stolen.
- For more information about keeping your personal information secure, view our security FAQs: [unfcu.org/frequently-asked-questions/security](https://unfcu.org/frequently-asked-questions/security)

