

# FMFCU's SECURITY NEWSLETTER



ALERTS | EDUCATION | PREVENTION

The security of our members' personal information and financial accounts is a top priority at FMFCU. As reports of scams and fraud attempts continue to increase, we want to ensure all members stay educated and alert to avoid becoming a victim.

## STAY ALERT FOR SCAMS



### MOST COMMON IMPOSTER SCAMS



#### CREDIT UNION IMPERSONATIONS

##### How it Works

- Member receives a call or text about suspicious card activity
- Claims to be from FMFCU's fraud department
- Convinces to reply with personal information to access account

##### Protect Yourself

- Hang up immediately
- Contact FMFCU directly to validate
- Never respond or click on links

#### FAMILY EMERGENCY SCAMS



##### How it Works

- Pretends to be a family member

##### Protect Yourself

- Hang up and don't reply to texts

- Says they need money for an emergency
- Asks for payment immediately through gift card or wire transfer

- Reach out to family member on their direct number
- Never send money over the phone
- Don't trust the voice – it can be spoofed



## GOVERNMENT IMPERSONATIONS

### How it Works

- Email, call or text appearing from government agency
- Claims you owe money to the IRS
- Threatens legal action if payment is not sent

### Protect Yourself

- Don't trust caller ID
- Verify directly with IRS
- IRS will only contact via direct mail

## ROMANCE SCAMS



### How it Works

- Creates fake dating profile
- Contacts through social media
- Manipulates by expressing love interest in order to receive money

### Protect Yourself

- Stop communication immediately
- Never send money or gifts to someone you haven't met in person
- Reverse image search of profile pictures



## TECH SUPPORT SCAMS

### How it Works

- Pretends to be a tech from well-known company
- Claims to offer legitimate technical support
- Pop-up windows can appear on your computer screen

### Protect Yourself

- Real security warnings and messages will never ask to call a phone number
- Hang up and don't click into pop-ups on computer
- Never screen share or give out credentials

## FOUR BEST PRACTICES TO AVOID IMPOSTER SCAMS

**1 – NEVER CLICK ON LINKS IN UNEXPECTED MESSAGES**

**3 – DON'T GIVE OUT INFORMATION OR PAYMENT OVER THE PHONE**

## RECENT SCAM ALERT – E-ZPass Phishing Scams



### How the Scam Works

- Targets E-ZPass account holders
- Text message from "PA Turnpike Toll Services"
- Alerts of outstanding account balance
- Asks for financial information
- Sense of urgency or coming soon late fees

### Protect Yourself

- Never click on links
- Do not reply to message or provide payment
- Only use approved methods to check accounts

[READ MORE](#)

Stay up-to-date with  
the latest information in  
FMFCU's Security Center

[More Info](#)



**FRANKLIN MINT  
FEDERAL CREDIT UNION**  
*The Credit Union of Choice!®*

Follow Us: [f](#) [X](#) [in](#)