



FAMILY AND COMMUNITY HEALTH

DIGITAL CITIZENSHIP & ONLINE SAFETY

Clara Cofield
Waller County Extension
Family and Community Health

PROTECTING PERSONAL INFORMATION

Risks of Sharing Personal Data

Sharing sensitive information online can expose individuals to identity theft and cyber attacks by malicious actors.

Strong Password Usage

Using strong, unique passwords for each account increases security and reduces the risk of multiple account breaches.

e.g., My first car was a Toyota in 2009! = MfcwaTi2009! Another example: "Let's have dinner at 8:00 p.m." which can become Lhd@800pm

Two-Factor Authentication Benefits

Two-factor authentication adds an extra verification step, making unauthorized access harder.

Real-World Example

A student sharing personal info on a public forum became a phishing attack target.



A POST THAT WENT TOO FAR

What Was Shared

A high school student posted a first-day-of-school photo with their ID badge clearly readable, standing in front of their home with their house number visible as well.

How It Was Used

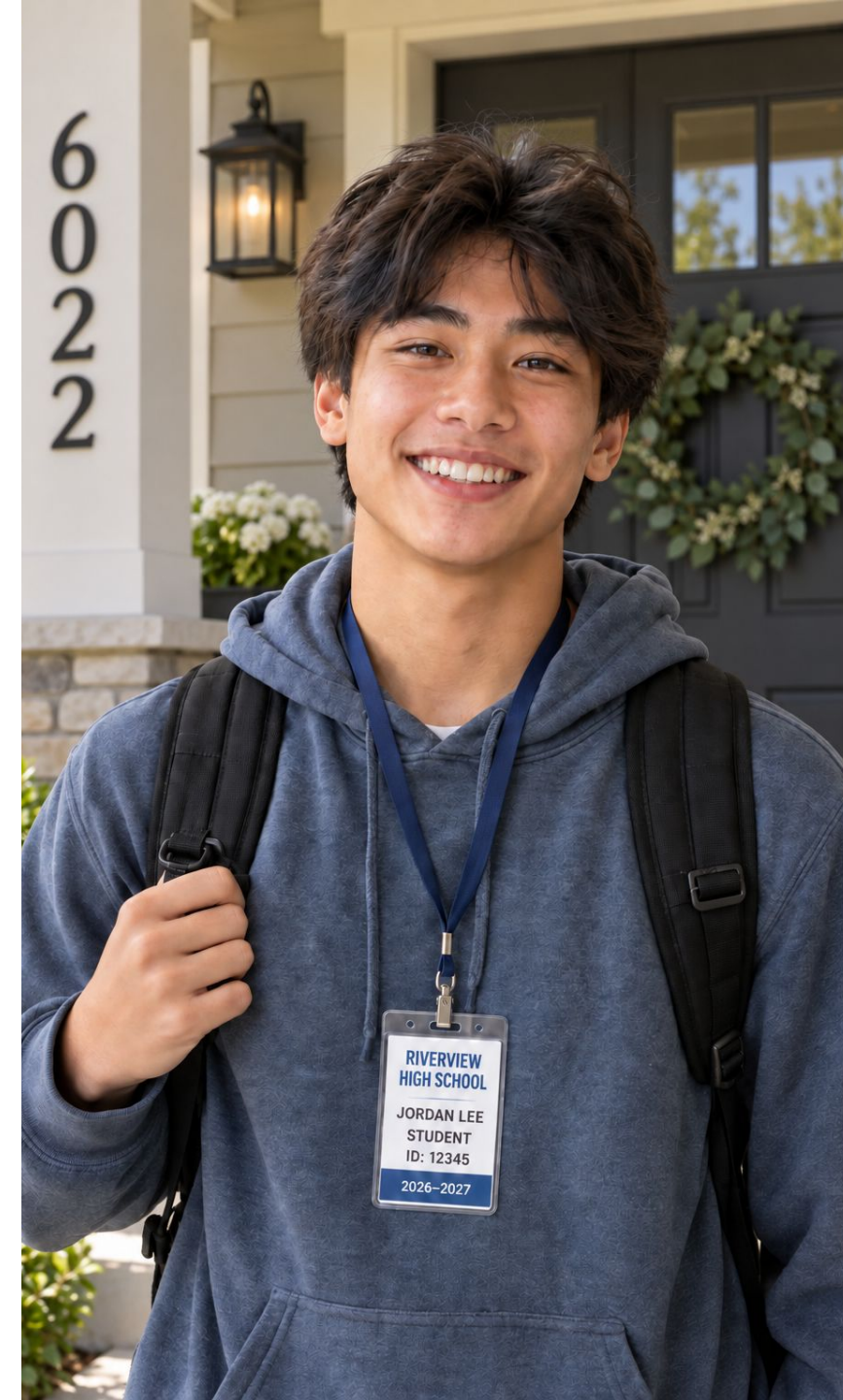
Within days, scammers messaged the student posing as school staff, using the ID number and address to sound legitimate and ask for family financial details.

The Damage

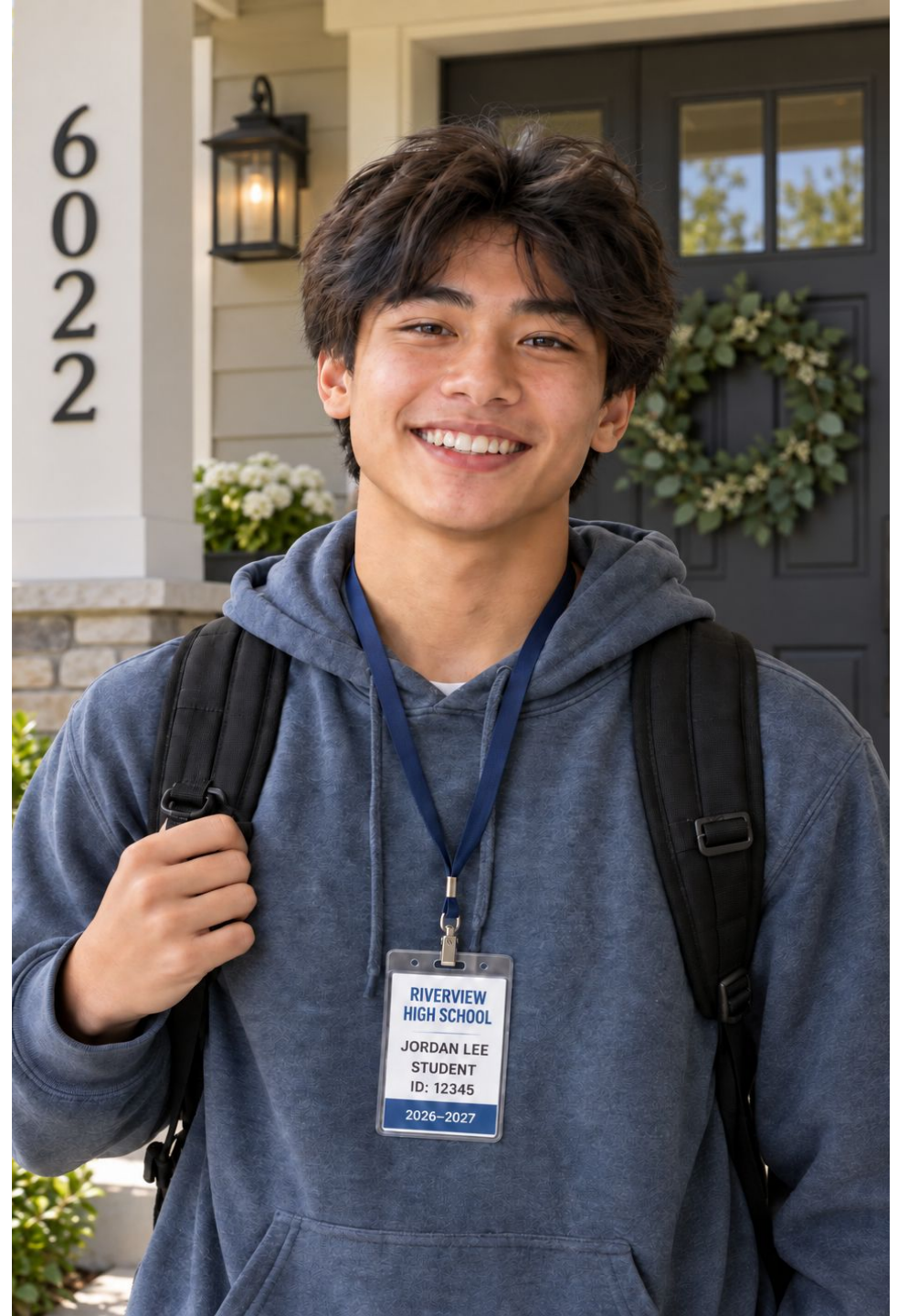
The information fed a phishing attempt on the family, and the post had already been copied and shared far beyond the student's friends list.

The Takeaway

Small details add up. Blur ID badges, skip location clues, and remember anything posted publicly can be saved by strangers forever.

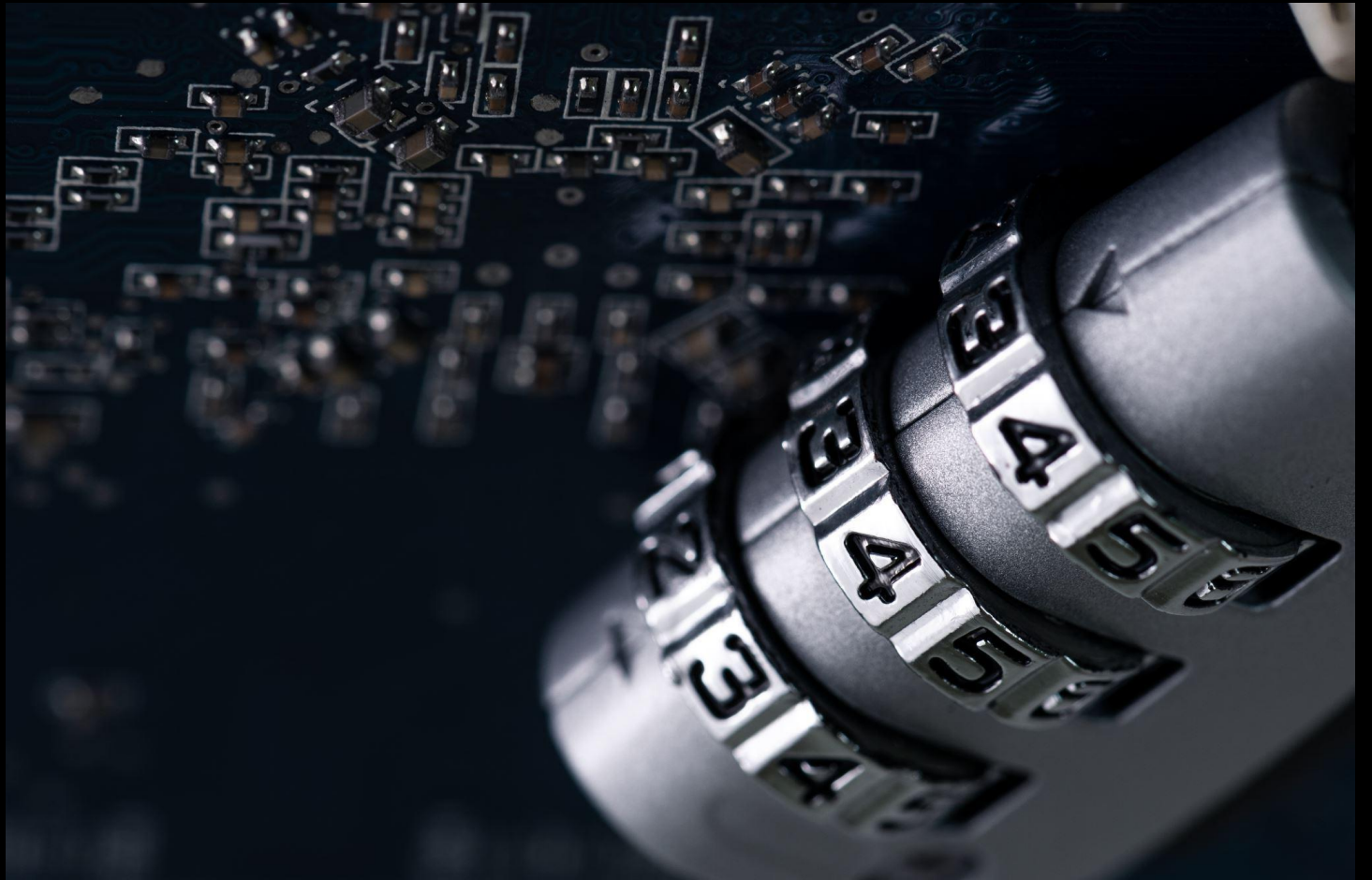


SAFE POSTING



PUBLIC OR PRIVATE

Full name
Birthday
Favorite restaurant
Home address
Work email
Passwords
Kids' school name
Vacation photos
Phone number
Hobbies
Credit card number
Health conditions



SOCIAL MEDIA SAFETY

Importance of Privacy Settings

Setting profiles to private limits access to personal information to trusted connections only.

Caution with Friend Requests

Be wary of friend requests from unknown individuals to avoid scams and data theft.

Think Before Posting

Carefully consider what you share online, as posts can be permanent and widely seen.

Real Life Consequences

Sharing sensitive information like vacation plans can lead to real threats such as burglary.



CYBERBULLYING PREVENTION

Forms of Cyberbullying

Cyberbullying includes hurtful messages, public shaming, and harassment on digital platforms.

Reporting and Blocking Bullies

Individuals should report and block bullies on social media to maintain a safe environment.

Retaining Evidence

Saving screenshots and messages helps when seeking help or taking further action against bullying.

Seeking Support

Open communication with trusted adults and counselors provides guidance and emotional support.

**SAVE
BLOCK
REPORT**



**SAVE
BLOCK
REPORT**

IS IT CYBERBULLYING?

Someone posts an embarrassing picture of a classmate without permission and others start laughing in the comments.

A friend disagrees with your opinion in a comment but does not insult you.

A group chat keeps excluding one person and sends mean messages about them every day.

Open communication with trusted adults and counselors provides guidance and emotional support.

**SAVE
BLOCK
REPORT**



**SAVE
BLOCK
REPORT**

PROTECT YOUR YOUTH WHILE GAMING

Set up Safety and Privacy Controls

Enable parental controls, tighten privacy settings, and protect in-game purchases so children don't share personal details or spend money without permission. Teach kids how to report and block abusive users.

Use Ratings and Know the Content

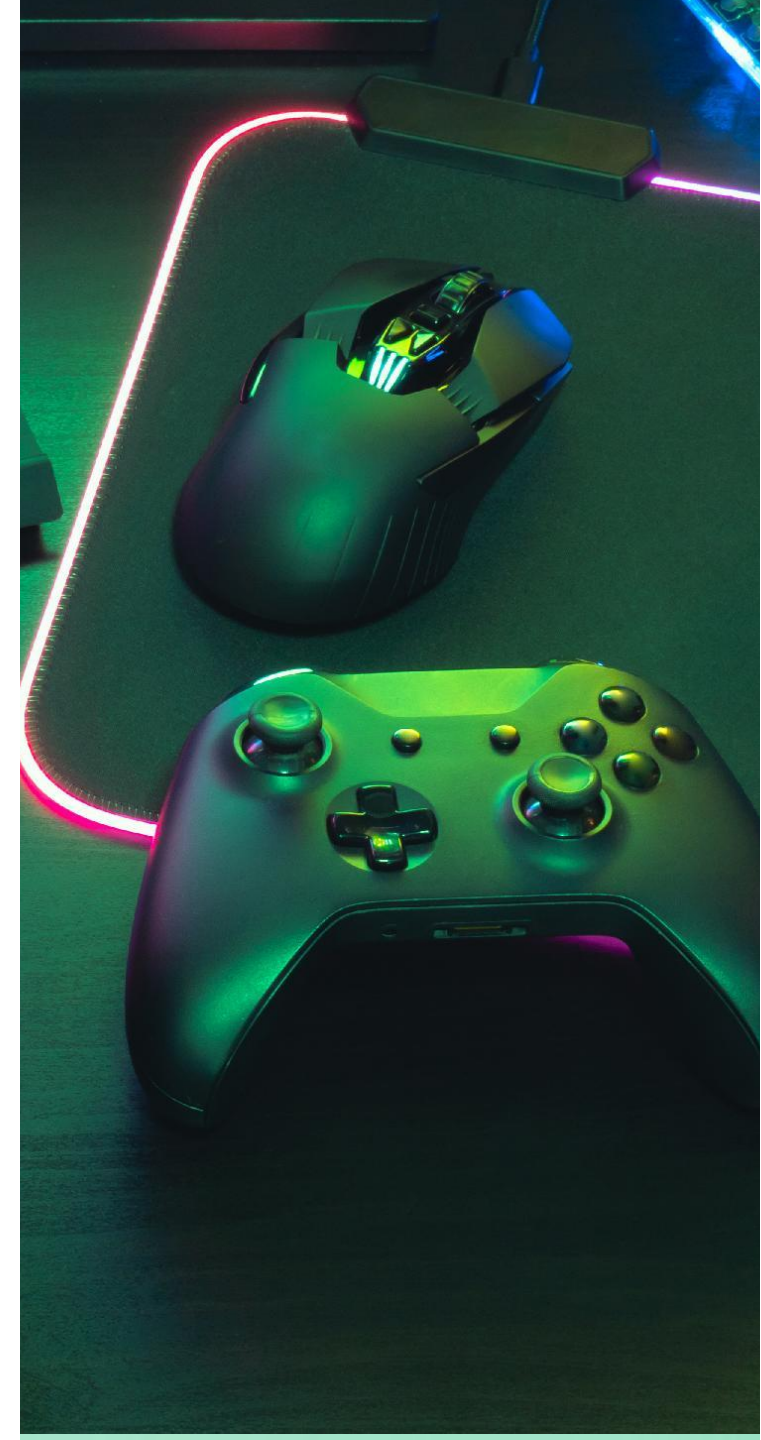
Check ratings! They tell you whether a game's themes are age-appropriate, but they don't show who your child might meet while playing.

Balance Gaming with Life

Encourage regular breaks and additional hobbies.

Stay Connected and Talk About Online Friendships

Talk regularly about who they play/chat with and what to do if they feel uncomfortable or come across something to report. www.CyberTipline.org or 1-800-THE-LOST®.



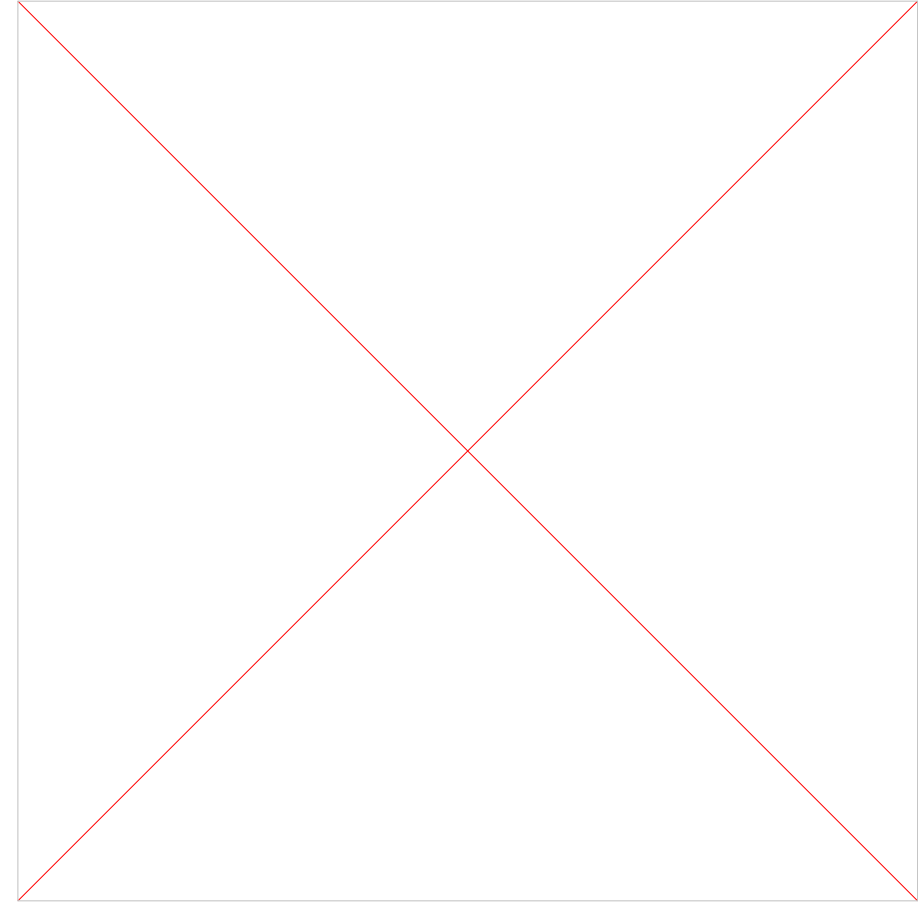
WHAT YOUR YOUTH SHOULD DO IF THEY SEE SOMETHING UNSAFE ONLINE

S – Stop

T – Tell an adult

O – Only talk to people you know

P – Protect your information



RECOGNIZING ONLINE THREATS

Common Online Threats

Phishing emails, corrupted links, and deceptive messages are frequent online threats targeting sensitive data.

Indicators of Phishing

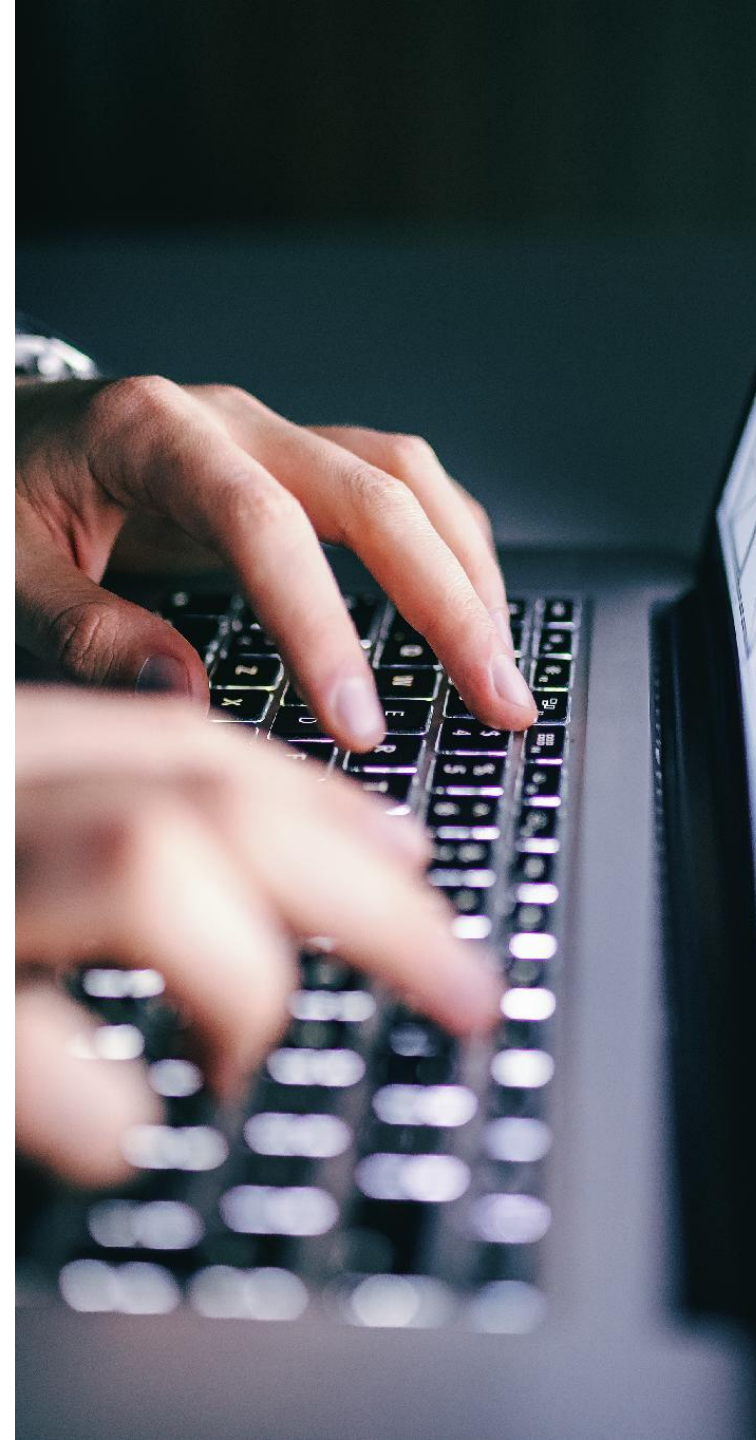
Urgent language, spelling errors, and suspicious links are key signs of phishing attempts to watch for.

Preventive Measures

Keeping antivirus software updated helps detect and block online threats before they cause harm.

Antivirus Software Should:

A user fell victim to a fake bank email, highlighting the need for vigilance and skepticism online.



PHISH OR REAL — CAN YOU SPOT THE SCAM?

URGENT! Your bank account has been locked. Click here immediately to verify your identity: www.bank-help-rite-now.com

Your Amazon package has shipped! Track it here: amazon.com/trackorder

Dear user, We notice unusual login attempt from your account. Please verify immediately

Congratulations! You've won a \$500 gift card! Just click [here](#) and enter your email and password to claim.

Your doctor's office has confirmed your appointment for Tuesday at 3 PM

Your package is delayed.
Track it here: tracking.parcel-service.com/XYZ123



RESOURCES:

Internetmatters.org - Game Safe Digital Guide, The ABC online safety checklist (by age)
www.CyberTipline.org or 1-800-THE-LOST®.

FTC.gov - Federal Trade Commission (Advice and Guidance Tab)

Netsmartz.org

Commonsensemedia.org - Parent Guide, Tips and FAQs

Waller County Extension Office

Clara Cofield
Waller County Extension
Family and Community Health Extension Agent
clcofield@pvamu.edu
979-826-7651



FAMILY AND COMMUNITY HEALTH