Healthy Aging Education Series

"Cyber Security – What's Lurking Now"

DATE: December 3, 2025
SUMMERVILLE FAMILY HEALTH TEAM

Asurtec

Asurtec Team Members

Cathy Timlin

Chief Operating Officer
with Asurtec Technology Solutions

Bill LeBlanc

Chief Finance Officer
with Asurtec Technology Solutions

TODAY'S TOPICS

01. Top Scams Facing Older Adults

02. Simple Habits to Stop Most Cyber-attacks

03. Banking and Money Protections

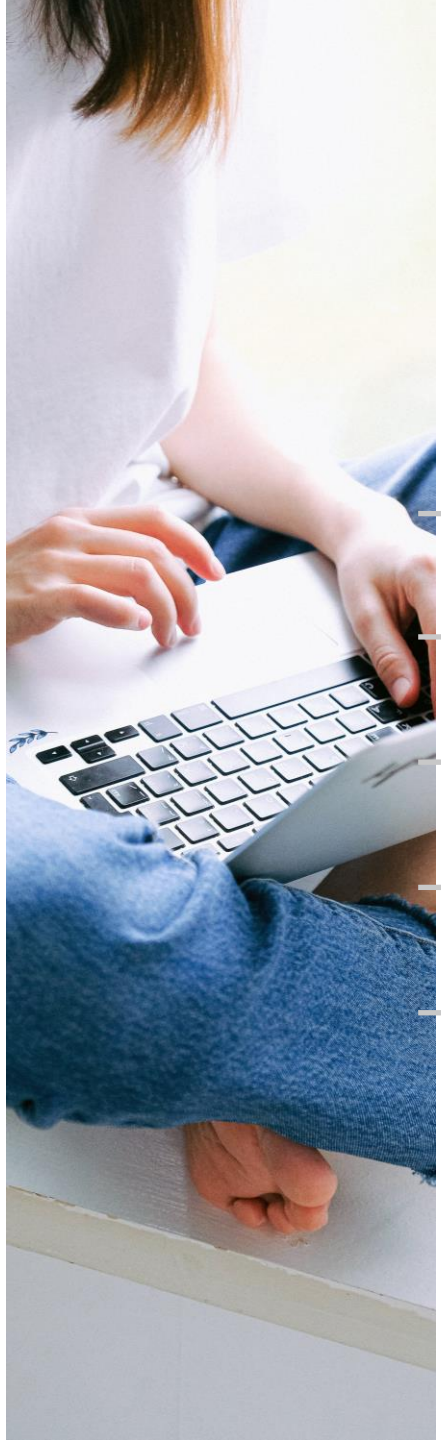
04. Phone and Text Safety

05. Phishing

06. What to Do after a Suspected Scam

Current TOP SCAMS

CYBERSECURITY

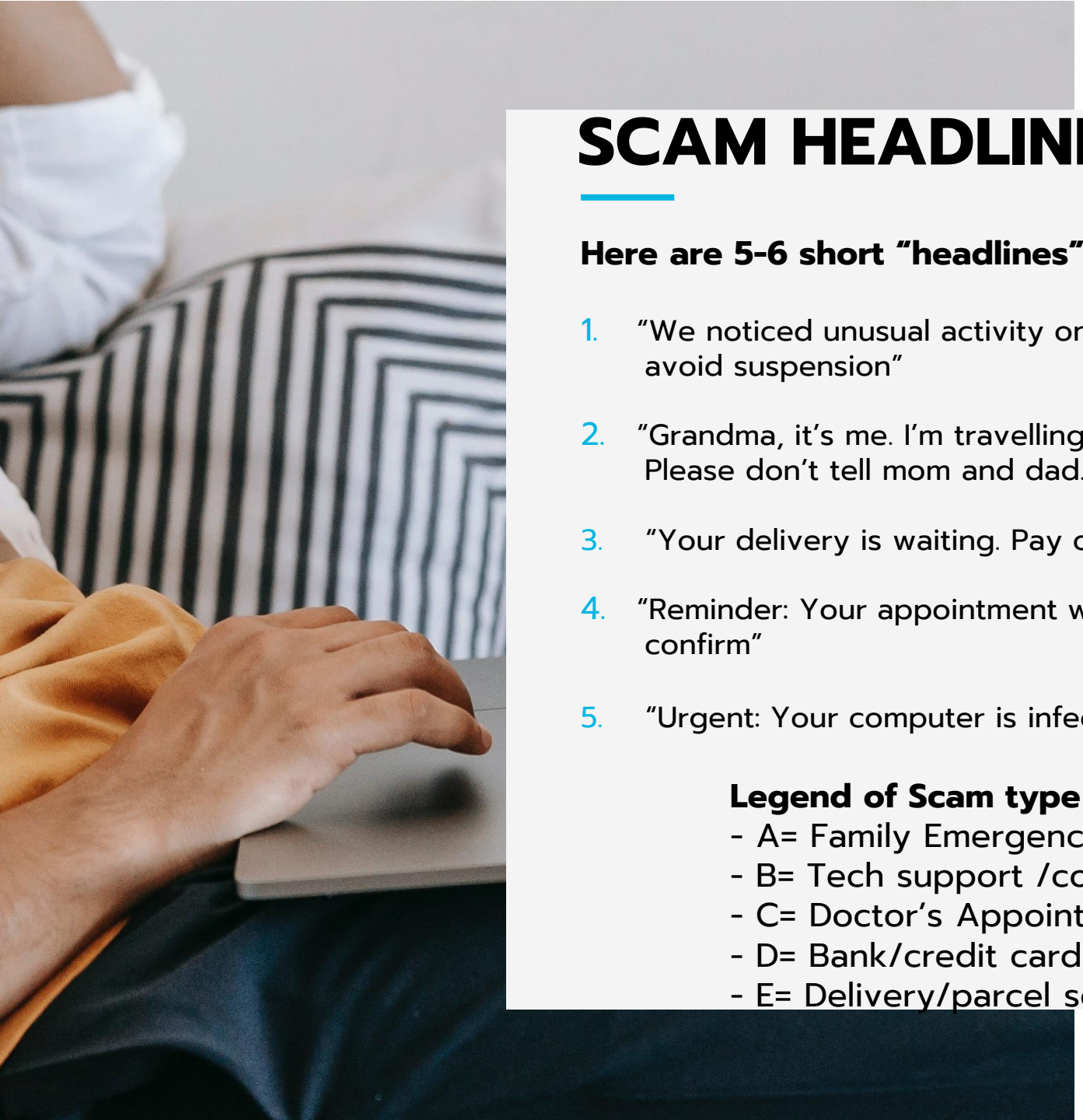


Know your *current* Top Scams

1. Grandparent Scam
2. Government, bank and tech-support impersonation
3. Romance scams
4. Investment & crytpo scams
5. Service & tech support scams

Golden Rule: If money, secrecy or urgency is involved...stop hang up and independently verify using a phone number or website you already trust.

Asurtec



SCAM HEADLINES

Here are 5-6 short "headlines"

1. "We noticed unusual activity on your card. Verify your account within 24 hours to avoid suspension"
2. "Grandma, it's me. I'm travelling and my wallet was stolen. Can you send money? Please don't tell mom and dad."
3. "Your delivery is waiting. Pay customs fee now to avoid return."
4. "Reminder: Your appointment with Dr. Singh is tomorrow at 2:30 pm. Reply YES to confirm"
5. "Urgent: Your computer is infected. Call Microsoft Support as 1-800-XXX-XXXX"

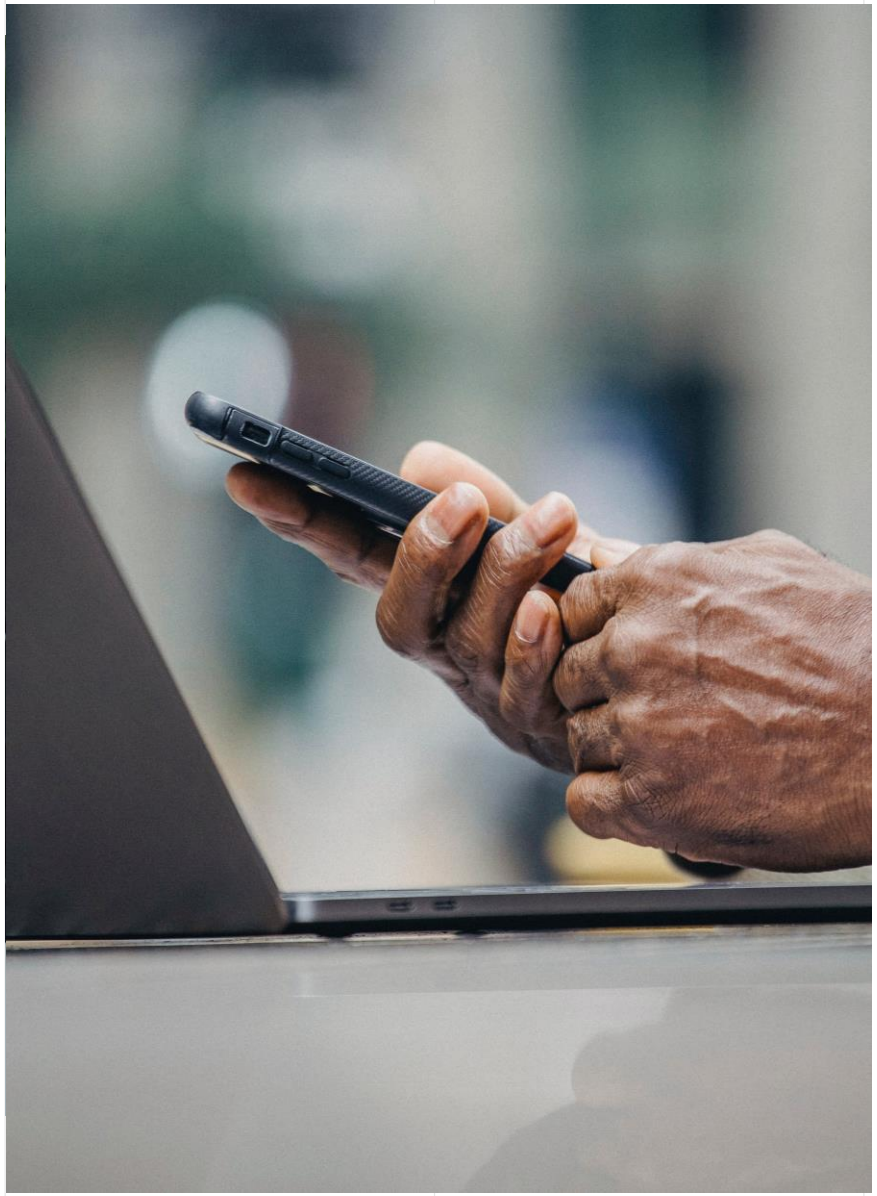
Legend of Scam type

- A= Family Emergency
- B= Tech support /computer scam
- C= Doctor's Appointment Reminder – (could be real)
- D= Bank/credit card scam
- E= Delivery/parcel scam

Asurtec

SIMPLE CYBER HABITS

Asurtec



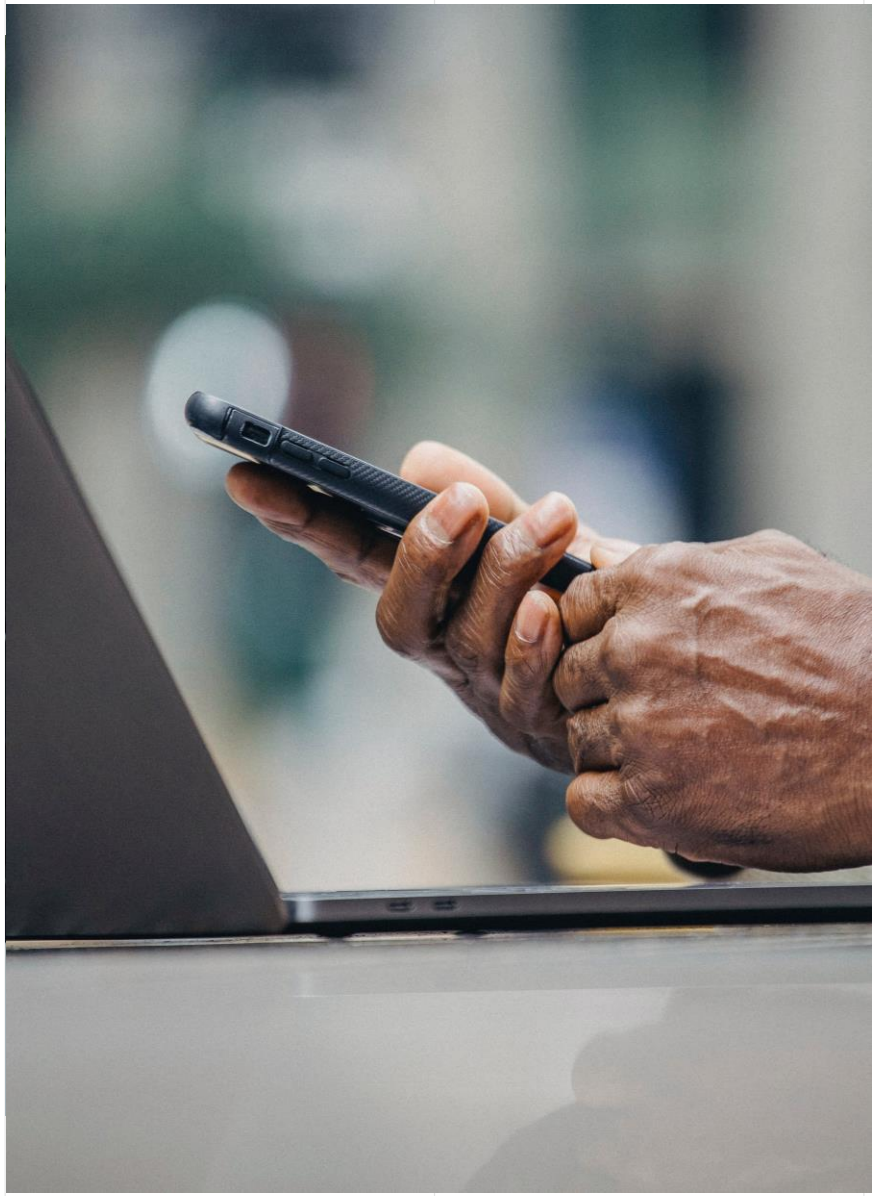
Good Cyber Habits

A. Passwords **(F6r*TP8)**

- Use strong, unique passphrases that's easy to remember but hard to guess
  - i.e. three or four unrelated words that is easy to remember but hard to crack – Yellow*TrainGarden42Tree
- Use a password manager
- Never reuse banking / email passwords anywhere else

B. Turn on Multifactor Authentication (MFA) everywhere

- Especially: email, banking, social media, shopping
- Use text codes or an authenticator app when possible



Good Cyber Habits

C. Keep Devices up to date

- Turn on automatic updates for:
  - Phone, Computer, Browser

D. Be "link-skeptical"

- Don't click on links in unexpected emails, texts from banks, delivery companies or government
- If you're unsure:
  - Type the website address yourself
  - Or call the organization using the *official* site or your bank card

Banking & Money Protections

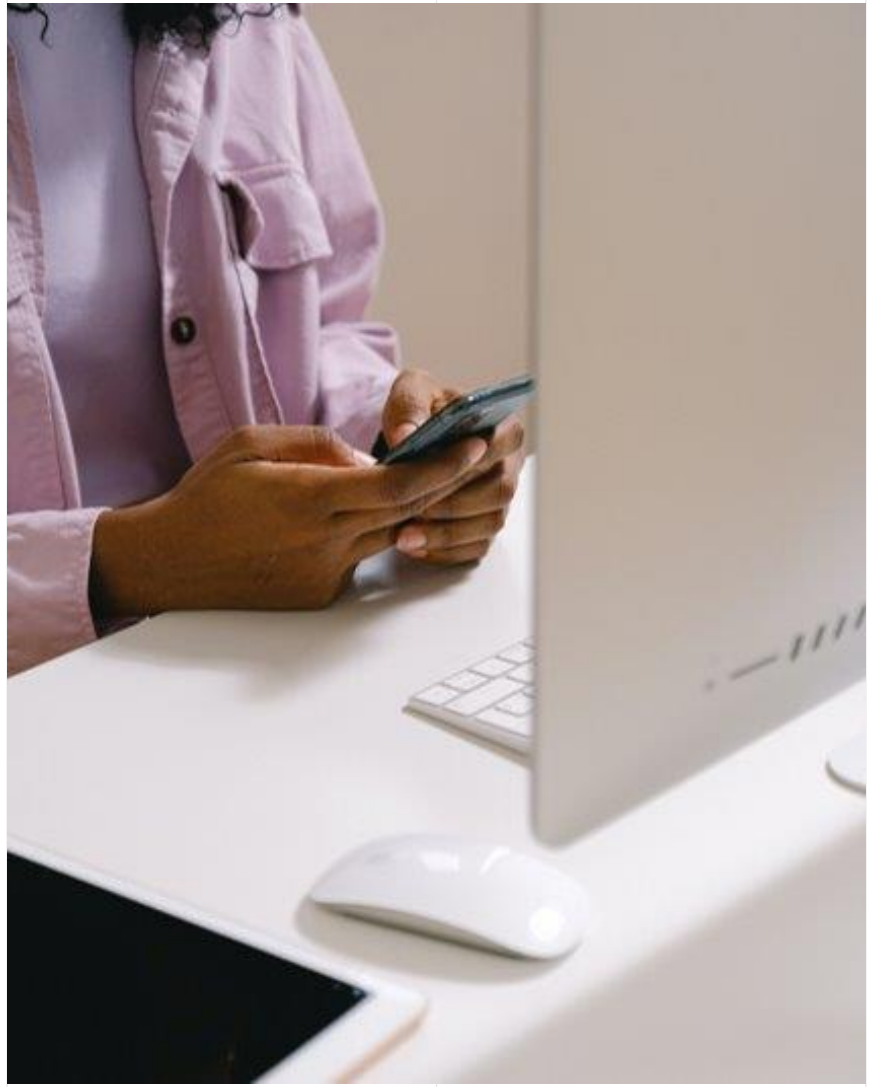
Banking & Money Protections

Financial-sector & Government Officials are really worried about older adult fraud

Top Tips

- Turn on bank alerts
  - Text/email alerts for large withdrawals, new payees, e-transfers, or foreign transactions
- Use credit monitoring or a fraud alert if:
  - You've been a victim
  - You know your information was in a data breach
- Consider daily-limit controls on e-transfers and debit purchases
- If something feels off:
  - Call the bank using the number on the back of your card (not the number from an email or text)

Phone & Text Safety



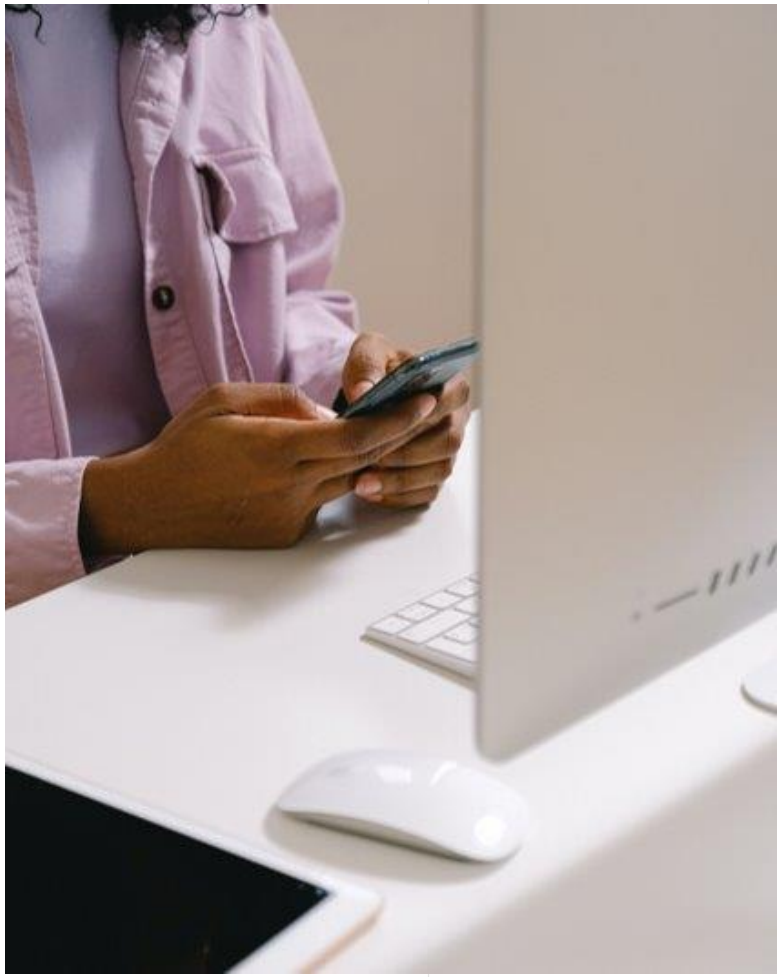
Phone and Text Safety

Most scams reach older adults by phone or text

If a phone call or text makes you feel rushed, scared, or secretive about money or information – PAUSE, HANG UP, AND VERIFY

Best Protections:

1. Let voicemail screen unknown numbers
2. Use Call Blocking
3. Never share:
    - Social Insurance Number
    - Full Date of Birth
    - Banking card # or PIN
    - One-time Passcodes sent by text
4. For grandchild/family emergency calls:
    - Have a family password for real emergencies



Tech Support Scams:

"Real tech support won't call you out of the blue, and real virus warnings don't tell you to phone a strange number"

Phone and Text Safety

Most scams reach older adults by phone or text

Tech Support Scams:

Best Protections:

1. Never call the number in a pop up
2. If they called you, assume it is fake
3. Don't let someone take control of your computer
4. New pay for "fixes" you didn't ask for
    - If someone you didn't call asks you to install any software so they can "help" – that's a scam sign"

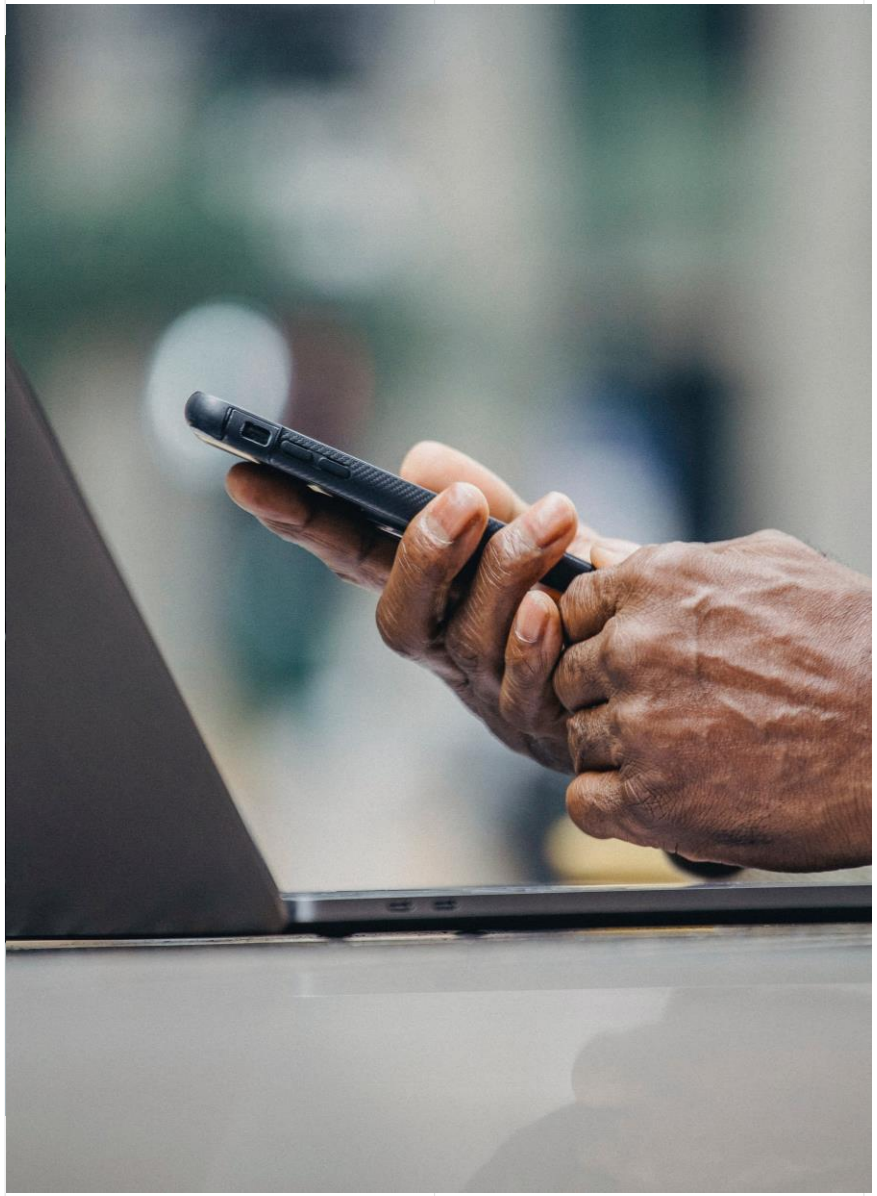
Simple Tips:

1. Hang up / close a pop up using Alt F4
2. Verify using a trusted source
3. Ask for help

Social Engineering Scams

What is Phishing and SmiSHing

Produced CSE Canada – Get Cyber Safe – "Phishing - Don't Take the Bait!"



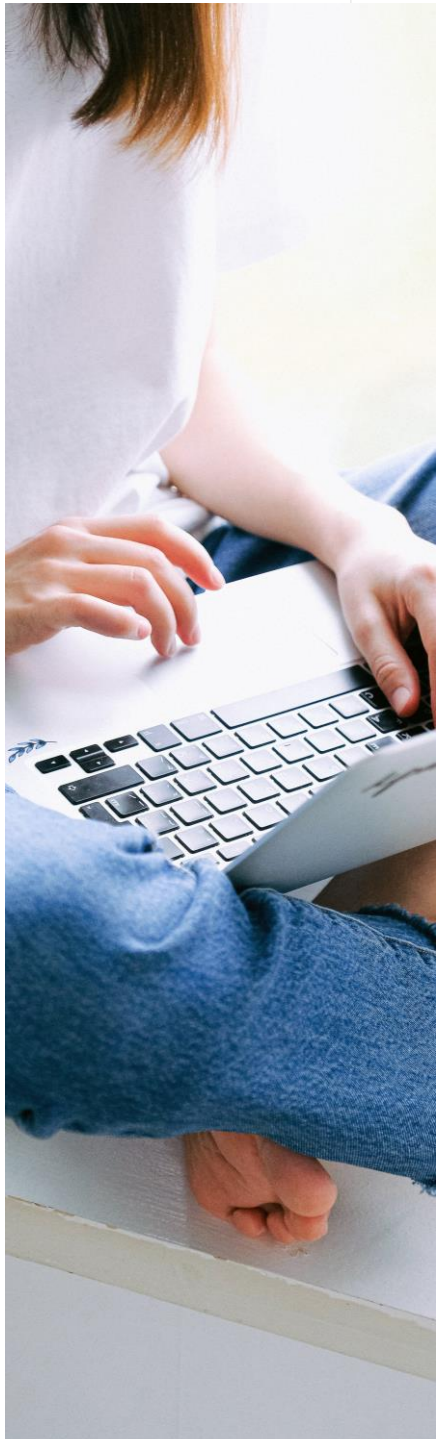
What to do after a suspected scam

If you suspect a scam:

- Stop communicating with the scammer immediately
- Contact the bank/credit card company and ask for:
  - Card cancellation
  - Charge dispute or reversal
  - Extra security or a new card
- Change passwords on email, banking and any reused accounts
- Report it:
  - Canadian Anti-Fraud Center (online or by phone)
  - Local Police (try to document what happened)
- Tell a trusted family member or caregiver

Personal Action Plan

CYBERSECURITY



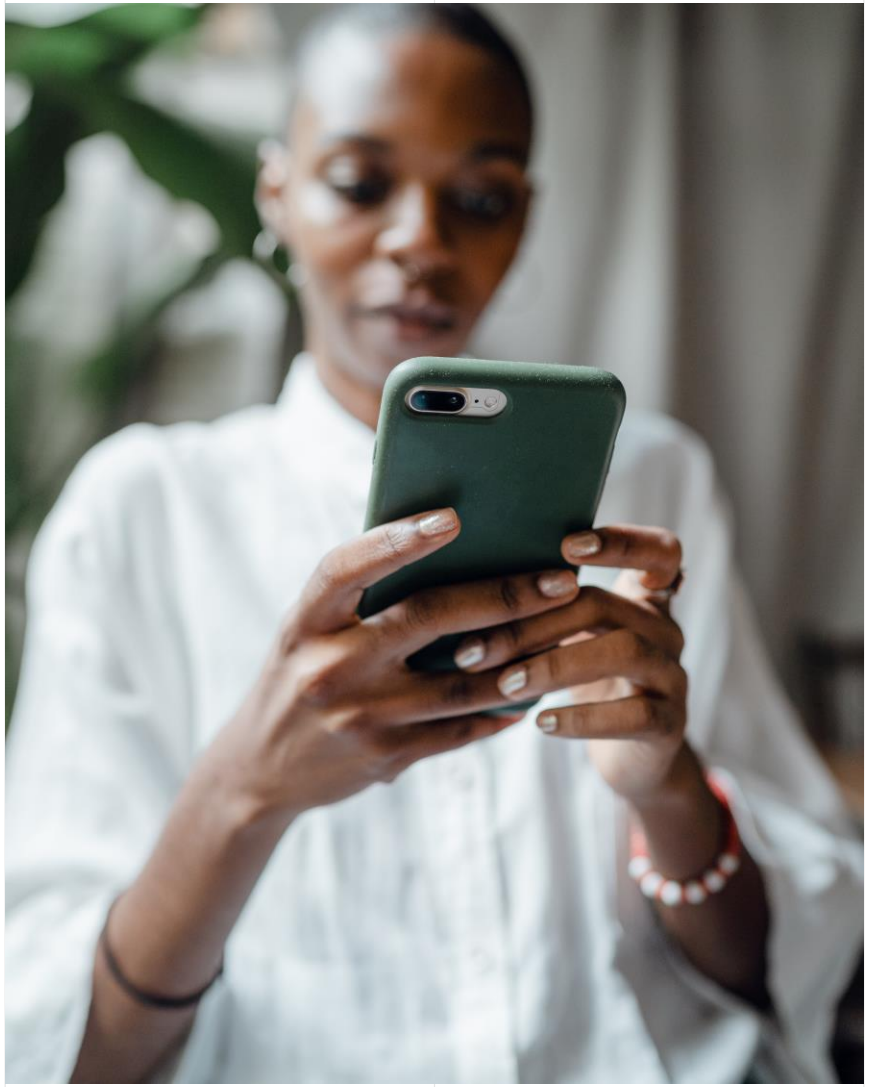
Your Cyber Safety Action Plan

- ❑ Ask my bank to turn on alerts
- ❑ Create a family password and share it with family members
- ❑ Let unknown calls go to voicemail
- ❑ Create a “scam folder” in my email
- ❑ Once a month, do a 10 min bank / credit card statement check look for transactions I don’t recognize
- ❑ Check my email “from” addresses before opening
- ❑ Post a reminder – “if it’s about money or panic – HANG UP & VERIFY
- ❑ Once a month I will read or watch one short item about scams

Asurtec

“Rules for Clicking”

Practical "Rules For Clicking" For Email and Social Media



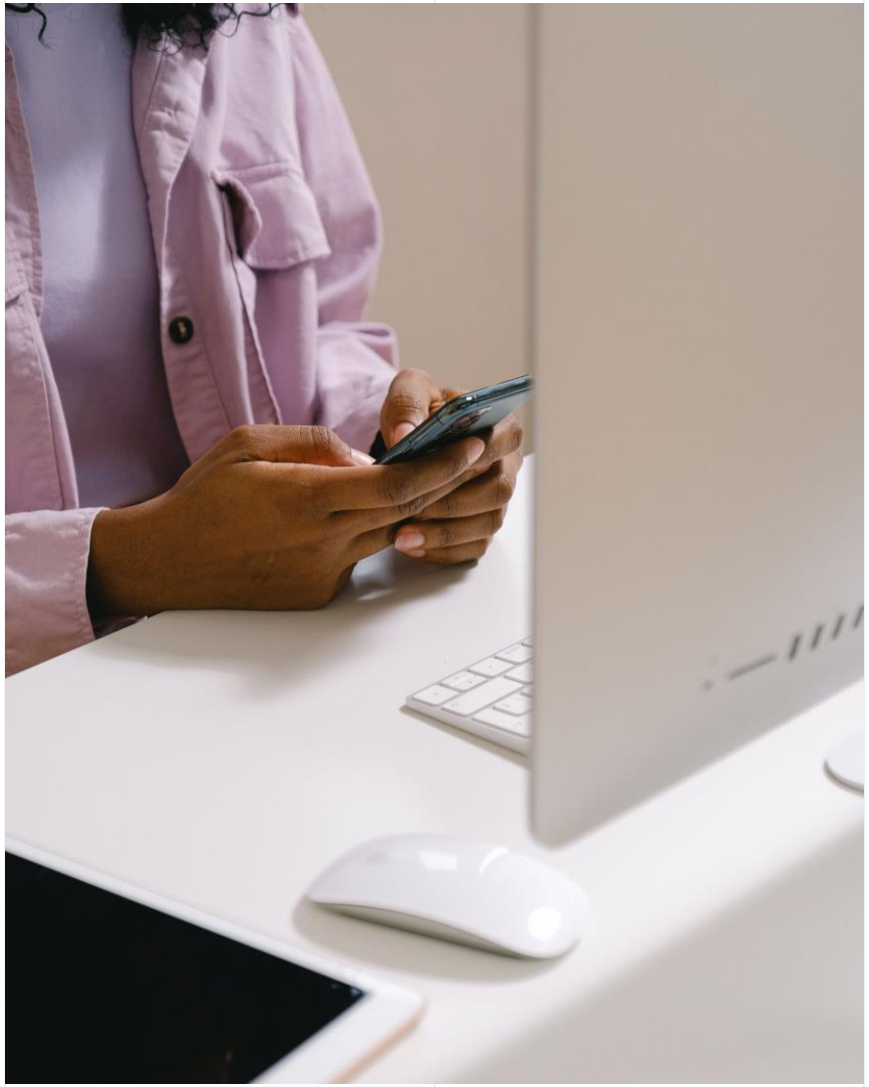
Canadian Cyber agencies – the patterns remain very consistent

Emails

- **Don't open attachments** you weren't expecting – especially invoices, shipping receipts, and documents to sign
- **Check the address,** not just the display name:
  - service@mybank.com – is ok
  - Mybank-security@hotmail.com is not

Social media

- Be cautious with "I saw this video of you…links
- Don't accept friend requests from people you don't actually know. If you think you are a friend double check before accepting



RESOURCES

Websites with Cybersecurity Resources

https://www.canada.ca/en/revenue-agency/campaigns/fraud-scams.html

https://publications.gc.ca/collections/Collection/JS62-85-1998E.pdf

https://www.getcybersafe.gc.ca/en

https://cba.ca/for-canadians/scam-prevention-toolkits

Here are a couple of recommendations to consider:

Password Managers

Bitwarden - https://bitwarden.com/

To report suspected or actual fraud please contact the - Canadian Anti-Fraud Center - https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

QUESTIONS?

THANK YOU FOR YOUR TIME