

# Consumer Scams

Understanding scams and mitigating the risks



## BANK IMPOSTER SCAM

### What is it?

A scam where the fraudster impersonates a bank employee to have the victim relay banking credentials, grant access, and/or send money. Similar schemes known as Authority Scams can have the scammer posing as the government, utility company or other technology and IT service providers.

### Scammer Goals

- Use fear or credibility to convince the victim they are a bank employee
- Persuade the victim to relay information such as One-Time Passcodes, access such as username and password, or send money externally

### Red Flags

- Presumed banker asks for banking credentials (usernames, passwords, etc.)
- Victim is asked to grant access to login device
- Victim is instructed to send money outside of bank to “secure funds”
- Victim is asked to lie



## ROMANCE SCAMS

### What is it?

A scam where the victim provides, receives or expects to receive money related to a romantic relationship they believe they are in— typically with someone they met online. Scammers will use many different social media platforms to meet and socialize with victims.

### Scammer Goals

- Gain the victim’s confidence
- Use the perceived relationship to convince the victim to act on their behalf (sending their legitimate funds, receiving/ sending illicit funds, etc.)

### Red Flags

- Relationship is long distance with love interest constantly unable to meet in person
- Sweetheart asks to utilize victim’s bank account to facilitate funds movement
- Sweetheart asks victim to lie (to friends, family, bank employees, etc.)



## ONLINE SALE SCAMS

### What is it?

A scam where the victim provides, receives or expects money related to an online sale. A person will typically give out their login or bank account information, believing this is an appropriate way to conduct transactions. They may also send their own funds to a scammer who fakes an item being sold.

### Scammer Goals

- Entice the victim with something that is often ‘too good to be true’
- Obtain access to victim’s bank account
- Convince victim to send funds for sale (which is fake)

### Red Flags

- Offer is too good to be true
- Buyer/Seller will not meet in person
- Items being sold use stock photos and may have conflicting information
- Buyer/Seller uses urgency to push for financial transaction



## WORK/JOB SCAMS

### What is it?

A scam where the victim provides, receives or expects money related to a job they have located online in which they believe they will be working from home. Fake jobs will include paperwork, payroll services, and more.

### Scammer Goals

- Convince the victim of employment
- Use the victim to transfer illicit funds (fraudulent checks, wires, etc.)

### Red Flags

- Unrealistic job descriptions or compensation; short or nonexistent job interview
- Job has victim using personal bank account to conduct “business transactions”
- Company is conveniently located far away from the victim



## REFUND SCAM

### What is it?

A scam in which a scammer pretends to be legitimate company issuing a refund to one of its customers. The refund turns out to be the victim’s own funds, which the scammers move from account to account. Victims will send the funds to scammer, not realizing it is their own money.

### Scammer Goals

- Pretend to be legitimate entity in order to obtain access to victim’s online banking
- Use internal transfers to convince customer of overpayment (resulting in the victim sending funds)

### Red Flags

- Caller pretending to be providing refund needs access to victim’s computer and online banking
- Caller pressures victim to ‘accept’ refund; they may use coercion or sympathy as well
- Victim is asked to send wire, buy gifts cards, etc., to fix ‘overpayment’

## WHAT CAN YOU DO?

- Exercise caution when meeting and interacting with people online
- Practice good social media etiquette
- Always do your research, ask questions, and know the risks of sending money
- Walk away when red flags are present; report fraud or suspicious activity