

Consumer Scams

Understanding scams and mitigating the risks



FIFTH THIRD BANK



	Romance Scams	Online Sale Scams	Work/Job Scams	Loan Scam	Refund Scam
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.	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.	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.	A scam where the victim believes they are obtaining a loan. These fake loans are typically found through social media and target people with poor credit. They often involve the customer giving out their banking credentials.	A scam in which a scammer pretends to be a 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	<ul style="list-style-type: none"> 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.) 	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> Convince the victim of employment Use the victim to transfer illicit funds (fraudulent checks, wires, etc.) 	<ul style="list-style-type: none"> Persuade the victim to seek money through fake loan Obtain access to victim's bank account or convince them to conduct illicit funds transfers 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.) 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Unrealistic job descriptions or compensation; short or non-existent job interview Job has victim using personal bank account to conduct 'business transactions' Company is conveniently located far away from the victim 	<ul style="list-style-type: none"> Loan found through individual on social media Victim is asked to provide online banking credentials in order to facilitate loan processing (this gives the scammer access to the account) 	<ul style="list-style-type: none"> 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 gift cards, etc., to fix 'overpayment'
What Can You Do?	<ul style="list-style-type: none"> 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 				