Understanding Fraud Scams

As businesses around the world have invested in cybersecurity, we have seen a shift in the way that fraudsters attack their victims. Scams have now emerged as the primary fraud risk for businesses, with criminals increasingly attempting to 'hack' people rather than machines. Here are three of the most common forms of scams that businesses need to be aware of:

	Phone	Text	Email
What is the Scam?	The attacker impersonates a bank employee and tricks their victim into disclosing security information	The attacker sends a fraudulent text message, which asks the victim to confirm a fictitious transaction	The fraudster impersonates a known contact and asks for a payment to be sent to a new bank account
Why are they successful?	The attacker creates a scenario where they appear to be offering help, so the victim is more willing to cooperate	The messages are customized to contain the victim's name/ company and appear to have been sent by the bank	The email looks genuine and will normally refer to an expected payment – such as a supplier invoice
How can you prevent it?	Citi Commercial Bank will not ask you to share your password, or a token-generated code, over the telephone	Citi Commercial Bank will not send you a text message to confirm a purchase or a transaction	Always call the sender – on a known/trusted telephone number – to reconfirm any changes in payment details

2128396 10/22