

PAYMENT SECURITY CHECKLIST

INITIAL REVIEW OF PAYMENT INFORMATION CHANGE REQUEST	
	Verify sender email address matches known contact. Look closely! Hover over (don't click) links to view and confirm legitimate URLs. Never open unsolicited attachments. Access websites directly instead of clicking links in the email.
VERIFICATION STEPS	
	FREEZE - No immediate action on any change request.
	LOOK OUT FOR RED FLAGS from the requester: Urgent language containing positive or negative outcomes if you don't act quickly, unusual communication style, attempts to bypass your organization's process, reluctance for in-person verification, claims their system is down or your usual contact is unavailable. Stop immediately if any red flags come up!
	REQUIRE any change in payment information to be done in person. Avoid taking change requests electronically or by phone.
	If in-person verification is actually not possible, contact the vendor/employee using an independently verified phone number (e.g. previous invoices, official databases, company website) and ask security questions about previous interactions that only the real vendor would know.
	SECONDARY VERIFICATION. Have a different staff member and the department that works directly with the vendor review verification attempts and confirm the change request.
	DOCUMENT all verification attempts.
PAYMENT PROCESSING	
	Separate staff handles payment initiation vs. approval.
	Compare new payment details against historical records.
	Flag any unusual payment amounts or destinations.
	Require management approval for changes to: Banking information, contact details, payment
	instructions.