BE AWARE OF SCAMS

WHAT IS A SCAM?

A SCAM IS A DISHONEST STRATEGY TO GET PEOPLE TO SHARE GIVE PERSONAL AND FINANCIAL INFORMATION.

PHISHING SCAM: SOMEONE PRESENTS TO BE AN INDIVIDUAL OR COMPANY YOU KNOW TO GET YOUR PERSONAL AND FINANCIAL INFORMATION.

FRAUD: A SUCCESSFUL SCAM

MOST COMMON TYPES OF PHISHING SCAMS:

HYPERLINKS SOCIAL MEDIA
TEXT (SMS) QR CODE
TELEPHONE EMAIL

COMMON SIGNS OF SCAM:

- PRESSURE TO MAKE A QUICK DECISION ON THE SPOT OR OVERNIGHT.
- ASKS YOU TO KEEP SITUATION CONFIDENTIAL AND NOT SHARE WITH FAMILY, FRIENDS, OR LOCAL AUTHORITIES.
- MESSAGES DEMANDING YOU TO CONTACT SENDER IMMEDIATELY.
- PROVIDE MONEY IN UNUSUAL FORMATS, LIKE GIFT CARDS, BIT COIN, AND PREPAID CREDIT CARDS.
- EMAIL FROM AN UNKNOWN SENDER WITH A LINK OR ATTACHMENT.
- EMAIL, TEXT, OR PHONE CALL REQUESTS FOR FINANCIAL INFORMATION (CREDIT CARD NUMBER, BANK ACCOUNT INFORMATION, AND PERSONAL IDENTIFICATION NUMBER (PIN)).
- EMAIL, TEXT, OR PHONE CALL REQUESTS FOR PERSONAL INFORMATION (SOCIAL INSURANCE NUMBER (SIN), DATE OF BIRTH, SECURITY ANSWERS, AND PASSPORT INFORMATION).

YORK UNIVERSITÉ UNIVERSITY

REPORT A SCAM

IF YOU THINK YOU HAVE FALLEN VICTIM OF A SCAM, TAKE THESE STEPS IMMEDIATELY:

1

STOP COMMUNICATING WITH SCAMMER RIGHT AWAY.

2

UPDATE YOUR ACCOUNTS

CHANGE PASSWORDS IN ANY ACCOUNT THAT WAS AFFECTED, INCLUDING SOCIAL MEDIA ACCOUNTS.

LET THE BANK AND OTHER COMPANIES KNOW THAT YOUR ACCOUNT MIGHT HAVE BEEN SCAMMED.

IF THE SCAMMER WAS ABLE TO ACCESS YOUR FINANCIAL ACCOUNT, IT IS IMPORTANT TO PUT AN ALERT ON YOUR CREDIT REPORT, WHICH IS A SUMMARY OF YOUR CREDIT HISTORY. YOU CAN DO THIS BY CONTACTING EQUIFAX CANADA OR TRANSUNION CANADA.

3

REPORT THE SCAM OR FRAUD TO YOUR LOCAL POLICE AND THE CANADIAN ANTI-FRAUD CENTRE.

GATHER ALL RECORDS YOU HAVE OF THE FRAUD OR SCAM (LETTERS, EMAILS, TEXT MESSAGES, RECEIPTS, CONTRACTS, ETC.).

AVOID TOUCHING DOCUMENTS THAT THE SCAMMER MAY HAVE TOUCHED, AND PROTECT THEM WITH A PLASTIC CASE OR COVER (IF THE SCAM OCCURRED IN PERSON)

KEEP A RECORD OF ALL OF YOUR ACTIONS SINCE THE FRAUD STARTED (INCLUDING DATES, TIMES, NAMES, AND CONTACT INFORMATION).

TIPS TO PROTECT YOURSELF FROM SCAMS:

- IGNORE AND BLOCK EMAILS FROM UNKNOWN SENDERS.
- IF YOU RECEIVE AN EMAIL OR MESSAGE FROM AN UNKNOWN SENDER, DON'T OPEN ANY ATTACHMENTS OR LINKS.
- BE CAREFUL WITH UPFRONT FEES. ASK AND UNDERSTAND WHY YOU NEED TO PAY FEES.
- IF A WEBSITE IS SECURE AND IS ASKING FOR CONFIDENTIAL INFORMATION, MAKE SURE TEH WEBSITE STARTS WITH 'HTTPS:' AND THAT THERE IS A SECURE SYMBOL (A CLOSED PADLOCK OR UNBROKEN KEY ICON).
- AVOID SENDING SENSITIVE/PERSONAL INFORMATION OVER EMAIL AND TEXT MESSAGES.
- NEVER PROVIDE YOUR PERSONAL, CREDIT, OR ONLINE ACCOUNT DETAILS WITHOUT CHECKING IF IT REALLY IS YOUR BANK OR ANY KNOW ORGANIZATION.

HELPFUL RESOURCES

YORKU REPORT PHISHING EMAIL: IF YOU RECEIVE AN EMAIL THAT YOU BELIEVE IS A PHISHING ATTEMPT OR SPAN, OPEN OR PREVIEW THE MESSAGE AND THEN CLICK THE "REPORT PHISHING" BUTTON.

YORKU PHISHING ALERTS: PHISHING AND SCAM ALERTS AFFECTING YORK UNIVERSITY STUDENTS, STAFF AND FACULTY.

CANADIAN ANTI-FRAUD CENTRE: COLLECTS INFORMATION ON FRAUD AND IDENTITY THEFT. THEY PROVIDE INFORMATION ON PAST AND CURRENT SCAMS AFFECTING CANADIANS.

SOURCES

ONTARIO.CA/IDENTIFY-SCAM-OR-FRAUD

CANADA.CA/EN/FRAUD-SCAMS

YORK UNIVERSITÉ UNIVERSITY