Fraud & Scam Prevention *Action Plan*

VtSBDC
VERMONT SMALL BUSINESS DEVELOPMENT CENTER

THE 3 MOST IMPORTANT STEPS TO PROTECT YOUR BUSINESS

1. Access Protection

Passwords

L00k@Thi$V3ry$tr0ngP@$$w0rd
"look at this very strong password"

- Create strong passwords for all software or systems that require a password
- They should have 12 or more characters, symbols, numbers, upper/lower-case letters, and avoid common words
- Use memorable sentences swapping letters for numbers and symbols as shown in the example above
- Alternatively, use a password manager (e.g. LastPass) which creates and stores strong passwords for you

Multi-Factor Authentication

- Enable multi-factor authentication (MFA) for all digital services used in your business, if available
- At the very least, use multi-factor authentication for all your digital financial services such as online banking
- Enable text message alerts from your bank and other financial services providers for suspicious transactions

2. Technology Protection

Updates

- Ensure that all software and systems are always up to date. When outdated, they are vulnerable to hackers
- Enable automatic software updates on all your devices, including computers, laptops, tablets, smartphones, etc.

Antivirus

- Use an antivirus on all your devices no matter what type of device it is (yes, Mac computers too!)
- Ensure the antivirus is always enabled and up to date, including built-in antiviruses (e.g. Windows Defender)

3. People and Business Protection

Protocols

- Create rules for financial transactions: *"At least two people must approve payments above XYZ dollars."*
- Create rules for access changes: *"Two people must approve changes of access credentials for online banking."*
- Train employees to handle urgent or suspicious requests using the SLOW method:
  - **S** – slow down, stop, and do not act!
  - **L** – log the contact by writing down their information and their request
  - **O** – one call to a primary contact to discuss and verify it
  - **W** – who is the authority to be informed if it is a scam? *(Call VT Attorney General's Office: 1-800-649-2424)*

Remediation Plan

- Have a list of emergency contacts in an accessible place in case your business falls victim to fraud or scam
- The list can include: your IT provider, lawyer, 24-hour bank or other financial service hotline, among others