Fraud and Scams
Are You Prepared to Protect your Business?

Business Resilience and Sustainability

Sergio Alvares
Statewide Advisor,
Strategic Projects - VTSBDC
sergio.alvares@vtsbdc.org
1. Our Relationship With Risk
2. Today’s Fraud and Scams
3. Our Behavior as the Weakest Link
4. How to Protect Your Business
5. Holiday Season Fraud and Scams
6. Q&A
Our Relationship With Risk

![Risk Indicator]

- Low
- Medium
- High

VtSBDC

Vermont Small Business Development Center
Our Relationship With Risk

What is the Limit of Our Ability to Assess Risk?

• There are infinitely more things we do not know than there are things we know.
• Imagine all human knowledge is a pie.
• Our individual knowledge is a paper-thin slice of this pie.
• There is great value in understanding our blind spots to avoid risks.
• Think about it: It is the car that you do not see coming that creates an accident.

Therefore, minimizing business risk:

• is not being prepared based on what you know.
• is considering all the things you are not thinking about that will hurt your business.

“Risk is what’s left over after you think you’ve thought of everything.” – Carl Richards
How Can Our Blind Spots Be a Great Asset?

• Our blind spots can be a great asset if we are willing to explore them

  “How can I think about things I do not know about?”

1. Be curious and investigate your main business areas
   • **People:** What are all the ways my employees can be scammed?
   • **Processes:** How can my business processes be exploited? (e.g. financial processes)
   • **Technology:** Are there opportunities for someone to manipulate my business technology unnoticed?

2. Get help from an outside business advisor
   • An external perspective is always helpful to identify our blind spots
   • **Others can see what we do not!**
Today’s Fraud and Scams
Today’s Fraud and Scams

What Are the Characteristics of 21st Century Fraud and Scams?

• Small businesses are a favorite target of fraudsters and scammers!
• Today, businesses rely on digital and online solutions for everything
• Fraud and scams are everywhere in the digital and online world
• Communication tools are some of the entry doors used by scammers
  • Voicemail
  • Text messages
  • Social media
  • Emails
• Employees responsible for external communication should be aware of the risks of being lured into a scam!
How Do Fraudsters and Scammers Operate?

- Today’s digital scammers are no different from those of the analog past: **All of them are after illegal financial gains**
- Their advantage today: easily accessing businesses from far away via the web and other communication means
- BUT... They need someone to inadvertently “open the door” for them
- They use many techniques to trick business employees
- **Scammers will always prefer a “low-hanging fruit”**
  - i.e., businesses that are the easiest targets
What Are the Most Used Digital Fraud and Scam Tactics?

• Preferred tactic: pretend to be someone else to **gain access** and **exploit** the victim

• Most of us are trusting individuals, and this very quality is exactly what scammers exploit

1. **Access:**
   • Emails and messages are sent to individuals in the business pretending to be someone they know and trust (phishing)
   • These messages will urge the person to either click on a link, download a file, or take some other action

2. **Exploitation:**
   • If a link is clicked or a file is downloaded, a computer can be locked by a malicious software, keeping files hostage and requesting payment for their release (ransomware)
   • Fraudsters may lure employees into taking actions such as changing online banking access, sending out checks, or making other types of payment to them
Our Behavior as the Weakest Link
Why Are We Humans the Weakest Link in The Digital and Online World?

• Machines are rule-based. Humans are emotional. That is what makes us unique, but also vulnerable
  • **Machine algorithm**: If safety features are enabled, then perform the task. Else, do not perform the task
  • **Human algorithm**: If asked nicely, then perform the task. Else, do not perform it (and make their life impossible... How rude!)

• That is why scammers will play on our emotions! Such as exploiting compassion or triggering a sense of urgency

• One way to combine the best of both worlds is to create internal protocols

• They add rule-based benefits to human operation:
  • “Two people must approve payments above XYZ dollars.”
Why Should Urgent Requests Always be Scrutinized?

• Often, fraudulent requests will have a sense of urgency
• It is done on purpose, so victims act hastily without questioning the authenticity of the sender and their request
• Every urgent request should raise a red flag 🚫
• Everyone should use the SLOW protocol to deal with urgent requests
  - 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?

“What is important is seldom urgent, and what is urgent is seldom important.” – Dwight Eisenhower
How Can Your Management Attitude Help Prevent Fraud and Scams?

• Preparedness is an attitude, not a skill
  • **Reactive management attitude:** act only when a problem appears and there is no way to ignore it
  • **Proactive management attitude:** organize themselves to maximize the chances that the problem never happens

• What do you prefer?
  • To deal with problems when it is too late?
  • Or ensure that you avoid problems that are avoidable?

• It is best to be proactive. But that is not how most of us operate

• **Ask yourself:**
  • Am I a reactive or proactive manager?
  • Is my management attitude making things easier or harder for me?

• **Recommendation:**
  • Make a conscious choice towards proactive management. The benefits are limitless
  • Remember, not choosing anything and letting chance manage your business is also a choice!

“It takes as much energy to wish as it does to plan.”
– Eleanor Roosevelt
How to Protect Your Business
What Are the Top Methods to Deter Fraud and Scams?

• Don’t be the “low-hanging fruit”! Discourage scammers from targeting your business by adding many obstacles

1. **Strong passwords** and **2-factor authentication** are very effective methods
   • 12+ characters, symbols, upper- and lower-case letters, and avoid common words
   • At the very least, use 2-factor authentication for financial services ([online banking](#))

2. Keep all **software up to date** and an **antivirus** running at all times
   • Enable automatic software updates on all your devices ([smartphones, laptops, etc.](#))
   • Use antivirus on all your devices and ensure it is always enabled/up to date (Mac users too!)

3. Most important, **train your employees** so they can avoid these risks
   • Create protocols: high value financial transactions, access changes, SLOW method
   • Remediation plan: have a list of emergency contacts in case the business falls victim to fraud
Are There Additional Methods to Protect a Business?

• Yes! You can always add more protective measures to your business

4. **Files back-up** can be vital in case they are kept hostage and a ransom is asked for
   - You can have a physical backup using a file storage device
   - Alternatively a virtual backup relying on a cloud storage service can be used

5. **Secure the router** that provides your business with internet access
   - Change its default password for a strong one
   - Create a separate network if customers need Wi-Fi access *(guest network)*

6. **Restrict access** to certain software and systems only to those who need to use it
   - E.g. Online banking: only those who make payments or use financial info should have access
   - Set different levels of access: full access, restricted actions access, read-only access, etc.
How to Get Prepared Without Being Overwhelmed?

• “This is too much. I must run a business AND do all that? No way!”
• It is only overwhelming if you see risk mitigation as an additional burden
• Think about it: we spend on avg. 1.5hs a day preparing and consuming food
  • 548hs each year = 23 days = one business month
  • BUT... we do not mind it nor resent the time it consumes. It is not seen as a burden
  • WHY? Because it is a necessary task for our survival
• Risk mitigation is also necessary for your business survival
  • If business preparedness becomes part of your business routine, it is no longer a burden
  • It is simply what you do!
• Start with small steps. Slowly expand your preparedness
How to Protect Your Business

Can You Give Me a Simple Action Plan to Start?

LINK: One-Pager Action Plan

3 Most Important Steps to Protect Your Business

1 – Access Protection
2 – Technology Protection
3 – People & Business Protection
Holiday Season Fraud and Scams
Yes, It’s Christmas! For Fraudsters and Scammers Too...

Businesses and employees are very busy and may not spot suspicious activities

1. **Alerts about compromised accounts**
   - Messages alerting that a bank or online shopping account was compromised are rarely true
   - Sometimes it looks, sounds, and feels like your bank is sending you a warning, but it is not!
   - Before clicking on a link from these messages, **contact the account provider to verify**

2. **Chargeback fraud**
   - Consumer makes an online purchase with a credit card and requests a chargeback after receiving the goods or services
   - Once approved by the credit card, a refund is issued and **the merchant may be accountable**

3. **“Holiday deals” for business services**
   - Someone calls offering an irresistible “holiday deal” for marketing and promoting services
   - It can be legitimate, but it can also be a scam. Get as much info as possible and research it
   - If it is legitimate, contact them back. **If it is not legitimate for sure, report it!**
Yes, The Threat is Real!

- Tech support imposter
- Fake IRS refund claims
- Service disconnection threats
- Business insurance scams
- …and the list goes on
Thank you! Questions?
General Business Questions and Updates

✉️ SBDC@VtSBDC.org
🌐 VtSBDC.org

Stay up to date on our social media (LinkedIn, Facebook, Twitter)

@VtSBDC

Useful Resources *(Office of the Vermont Attorney General)*

Consumer Assistance Program Scam Reporting Form *(Hotline: 1-800-649-2424)*

Scam Prevention Page

Consumer Assistance Program Blog