U.S. Small Business Administration

Small Business Owner's Checklist for Growth

Irene Gonzalez, Economic Development Specialist

Provided by:

U.S. Small Business Administration

Boise District Office

#1

Know Your Cash Flow – Have the Capital You Need

If you're making sales, then all is well – Right? The answer is NO - you can be making sales and not have cash flow.

Create a cash flow projection

Watch your financials weekly

Look for ways to get paid by customers faster

Research your business needs to obtain financing before you need it

Lay out incremental sales and spending in detail

Local bank or credit union

Consider an SBA loan

#2
Stand Out From the Crowd

Have a “unique value that customers want”. Your value is your benefits.

- Keep Adding Something New
- Become a Valuable Resource
- Separate Yourself from your Competition
- Promote the End Result
- Anticipate Change

- **Don’t confuse price and value**
- **Create a unique value proposition (UVP) and convey it to your customers**
- **Consider selling online**
- **Entertainment – Engagement – Education - Experience**

#3
Think Bigger

How are you going to grow and what are the steps necessary to make it happen?

- What's right?
- Where do the best opportunities exist?
- What resources are needed to get there?
- Ways to collaborate?
- Tapping into new sales and delivery channels?

- **Start with the easiest growth strategy first**: *Baby Steps*
- **Master inventory management**
- **Be prepared: Plan and manage your business**

#4

Know Your Customers — Very Well

- Stay responsive, connected, identify and rework every problem, and embrace new approaches.

- **Switch your mindset from being product-focused to being customer-focused.**
- **Cater to the wants and needs of your target customers**
- **Talk to 10 to 20 customers (at least monthly)**
- **What are people saying on social media**
  - **Post a comment that generates a response**
  - **Ask the same questions through all your social media channels**

#5
Test the Market

- Test the market with any new product or service idea.
- Get feedback from new and existing customers.

- **Focus group**
- **Give free samples**
- **Attend a fair or expo**
- **Be a sponsor (organizations – swag)**

#6

Staffing For Success

If the owner is trying to do everything themselves, it limits the possibility for growth.

Be the manager, not the technician

- Spend your time on what you do best — what is going to drive revenue
- Have a strong team

- **Attract the right applicants**
- **Spend money on salaries**
- **Personality vs. skill**
- **Set goals and provide training**

#7

An Engaging Business Culture

Create a culture that engages your staff, and your clients can really get behind.

- **Convey your vision**
- **Respect and recognition**
- **Offer good benefits and perks**
- **Value EVERY employee**

#8

Be Open to the Needs of Your Business

Vision Who you are – Core Values / Purpose-Cause-Passion-Niche

People Right people/right seats. Structure of organization

Data Scorecard / Measurables

Issues List all issues / Identify – Discuss – Solve

Process Documented – Follow through

Traction Execution of your vision

#9

Who is Your Yoda?

Entrepreneurs need to consistently be learners.

- Use the wisdom and insight of someone who is successful or can offer you lessons learned.

- **Ask people you admire**
- **Network with investors**
- **Business Consultants**
- **Surround yourself with positive influences**
- **Join organizations that can lead to collaborations**

www.idahobizhelp.idaho.gov

- Small Business Wizard

  (Local, State and Federal)
  - Taxes
  - Regulations
  - Licensing
  - Permits
- Resource Wizard
  - Agricultural loans and resources
  - Angel and venture capital resources
  - Bank loan programs
  - Business incubators
  - Chambers of commerce
  - Economic development organizations
  - Government procurement opportunities
  - Import/Export/International Trade assistance
  - SBA loan programs

Cybersecurity for Small Businesses

OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

Cybersecurity Tips for Small Businesses

Small employers don’t consider themselves targets for cyberattacks

- Due to their size
- They don't have anything worth stealing
- Have valuable information - employee and customer data, bank account information and access to the business's finances, and intellectual property
- Provide access to larger networks such as supply chains

MAKE
SMART SECURITY
YOUR BUSINESS AS USUAL

- Ç Business Plan
- Ç Marketing Plan
- Ç Cybersecurity Plan

IDENTIFY
• Asset Management
• Vulnerability Assessment
• Governance, Risk & Compliance
PROTECT
• Threat Prevention
• Access Control
• Data Security
DETECT
• Continuous Monitoring
• Anomaly Detection
• User & Application Awareness
RESPOND
• Incident Response
• Malware Analysis
• Forensic Remediation
RECOVER
• Continuity of Operations
• Disaster Recovery
• Threat Mitigation
CYBER SECURITY

Identify

- What needs protection in your business
- Common cyber attacks that may be used against your business
- The risks and costs of not being prepared for a cyber attack

Protect

- Train your employees to make smart decisions on electronic devices
- Use firewalls, encryption and strong passwords
- Actively assess and manage cyber risk

Detect

- Implement company policies
- Buy and regularly update antivirus software
- Teach employees to recognize cyber attacks

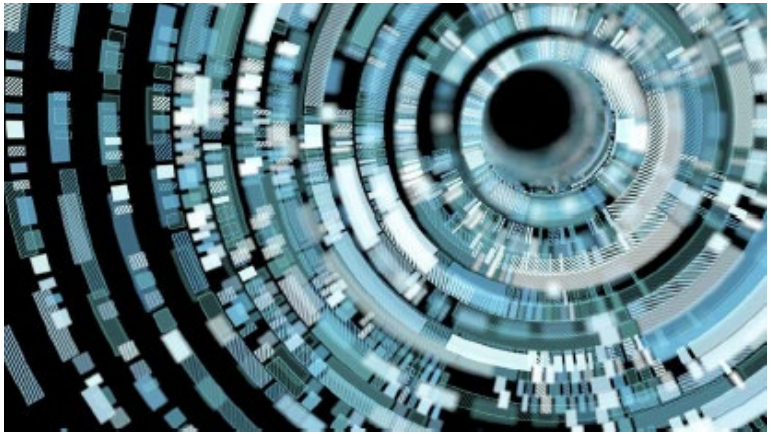
Respond

- Develop an Incident Response Plan
- Do a simple and low cost risk assessment for your business
- Actively manage your business's security risks

Cybersecurity threats are real and businesses must implement the best tools and tactics to protect themselves, their customers, and their data.

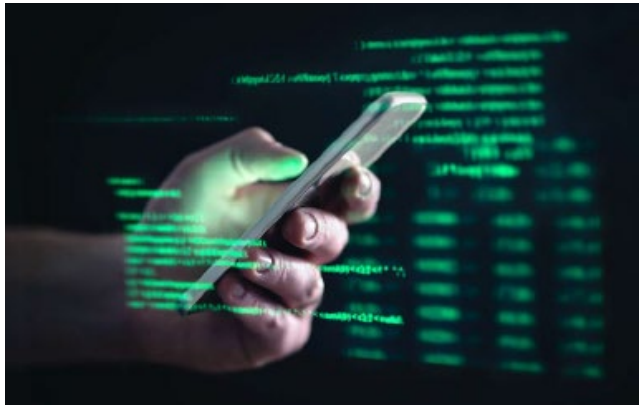
Train Employees in and Establish Security Principles

- Basic security practices and policies for employees.
- Use strong passwords
- Appropriate Internet use guidelines
  - Detail penalties for violating company cybersecurity policies
- Rules of behavior
  - Protect customer information and other vital data



Protect Information, Computers, and Networks From Cyber Attacks

- Keep clean machines
- Update Your Software
  - Apps, web browser, and operating system
- Set antivirus software to run a scan automatically after each update



Provide Firewall Security for Your Internet Connection

- A firewall is a set of related programs that prevent outsiders from accessing data on a private network.
- Make sure the operating system's firewall is enabled.
- If employees work from home, ensure their home system(s) are protected by a firewall.

Create a Mobile Device Action Plan

- Require users to password protect their devices
- Encrypt their data
- Install security apps to prevent criminals from stealing information while on public networks
- Procedures for lost or stolen equipment

Make Backup Copies

- Regularly backup the data on all computers
  - Automatically if possible, or at least weekly
  - Consider storing the copies off site
  - The cloud
- Critical data includes:
  - **Financial files**
  - **Human resources files** / PII (Personal Identification Information)
  - **Accounts receivable/payable files**
  - Word processing documents
  - Electronic spreadsheets
  - Databases

Control Physical Access to Your Computers and Create User Accounts for Each Employee

- Prevent access or use of business computers by unauthorized individuals
- Laptops are easy targets for theft or can be lost - lock them up when unattended
- Create separate user account for each employee and require strong passwords
- Administrative privileges given to trusted IT staff and key personnel

Secure Your Wi-Fi Networks

- Secured, encrypted, and hidden
- To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID)
- Password protect access to the router

Employ Best Practices on Payment Cards

- Work with banks or processors to ensure validated tools and anti-fraud services are being used
- Isolate payment systems from less secure programs
- Don’t use the same computer to process payments and surf the internet.

Limit Employee Access to Data and Information, and Limit Authority to Install Software

- Do not provide any one employee with access to all data systems.
- Employees should only be given access to the specific data systems they need for their jobs.
- Employees should not install any software without permission.

Passwords and Authentication

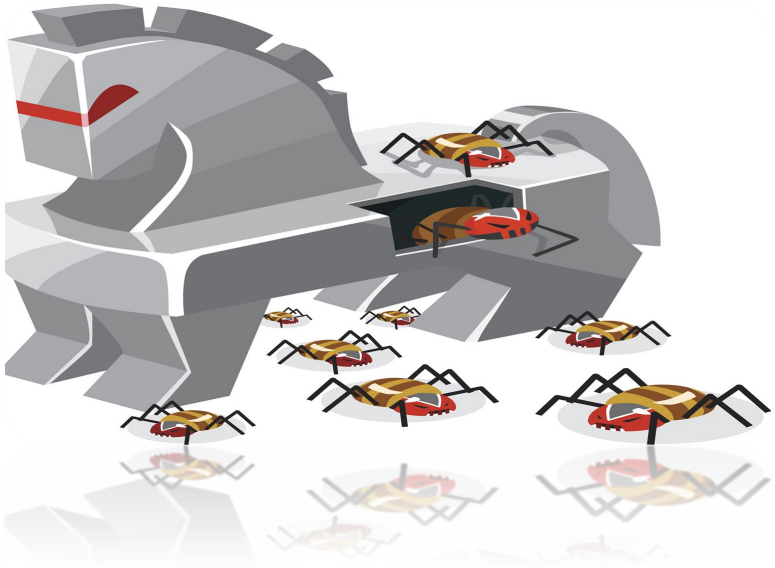
- Unique passwords - change every three months
- Consider multifactor authentication that requires additional information beyond a password
  - Security Questions
  - A code sent to another device
  - Biometric measure – fingerprint, eyes
- Check with vendors and financial institutions, to see if they offer multifactor authentication for your account.

crime
data
protection
phishing
web
internet
attack
virus
ransomware
information
privacy
crime
ransomware
trojan
data
online
virus
ransomware
crime
malicious
Malware
cyber
cyber
cyber
security
internet
software
online
protection
security
trojan
spam
phishing
network
trojan
spam
information
data
attack
spyware
virus
privacy
virus
technology
web
internet
malicious
software
attack
internet
spyware
malicious
technology
crime

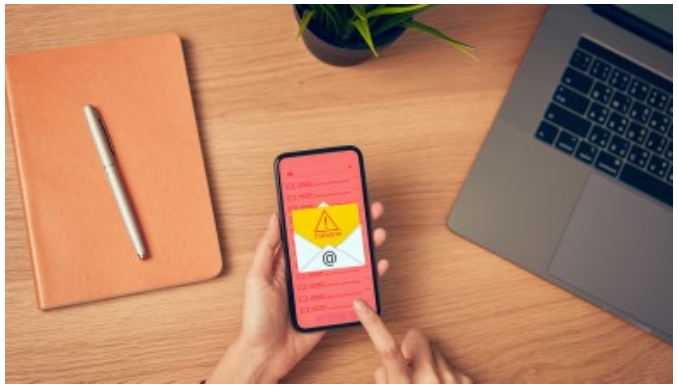
What is Malware?

Malware, short for malicious software, is a broad term used to refer to a variety of hostile or intrusive software:

- Computer viruses
- Worms
- Trojan horses
- Ransomware
- Spyware
- Adware
- Scareware
- And other malicious programs.



How Can You Be Infected?



- Malware can be installed by simply navigating to an infected website, opening an email attachment, or clicking on a social media link.
- Did you know that some malware can come from malicious text messages on your smart phone?
- Be careful of unsolicited text messages and emails.

What Are Some Possible Indicators Of Malware?

- Unwanted pop-ups
- Unfamiliar icons on desktop
- Suspicious hard drive activity
- Running out of hard drive space
- Unusual messages or programs that start automatically
- Unexpected system slowness
- New browser homepage, new toolbars and/or unwanted websites accessed without your input
- Crashes

Ransomware

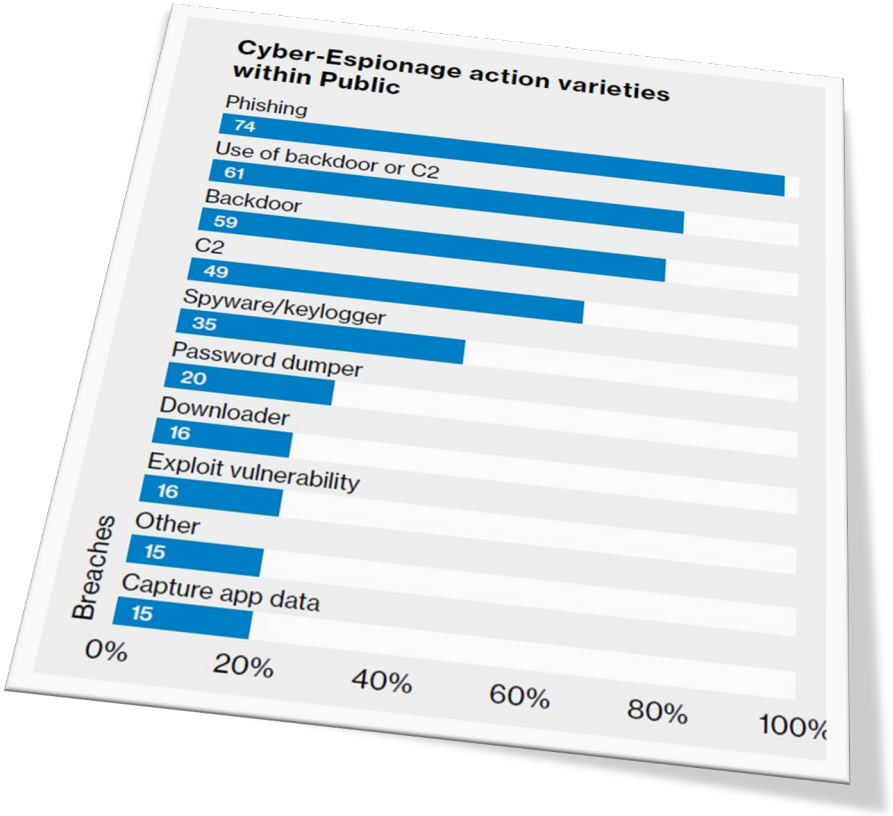
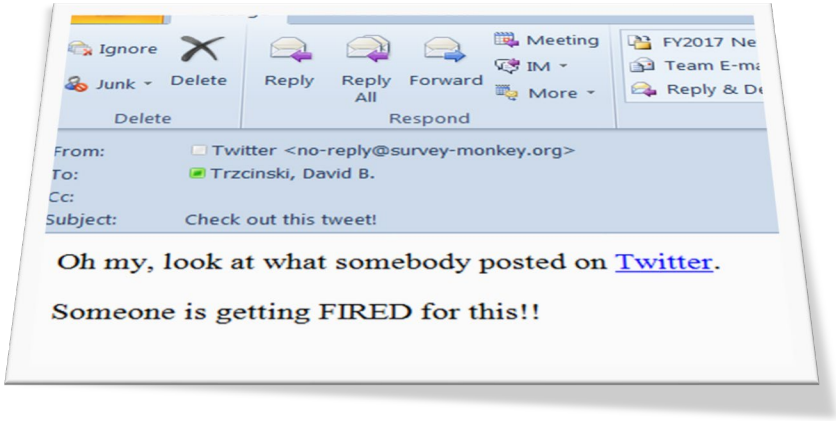
- A type of malicious software that infects and restricts access to a computer until a ransom is paid.
- Frequently delivered through phishing emails and exploits unpatched vulnerabilities in software.

Top 5 Types of Small Business Scams

1. Bank/ Credit Card Company Imposter
2. Directory Listing and Advertising
3. Fake Invoice/ Supplier Bill
4. Fake Check
5. Tech Support

Is Phishing Really A Big Deal?

- Emails appear as though they have been sent from a legitimate organization or known individual
- Entice users to click on a link or open an attachment containing malicious code.
  - After the code is run, your computer may become infected with malware



- Don’t click directly on links in emails, even if the sender appears to be known
- Verify web addresses independently
  - Contact your organization's helpdesk
  - Search the Internet for the main website of the organization or topic mentioned in the email.
- Exercise caution when opening email attachments.
- Be wary of compressed or ZIP file attachments.
- Social media, messaging services, and apps are increasingly being used to carry out attacks.