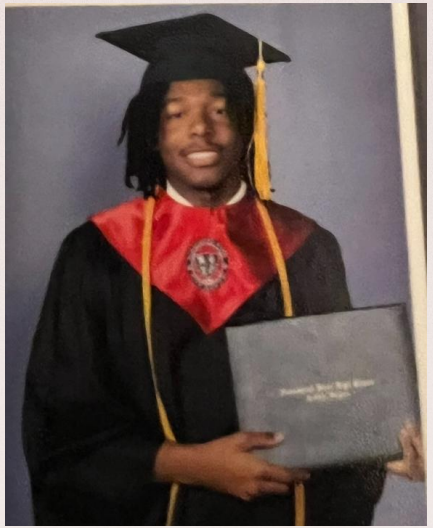
JenDore Cyber Assessmen t

Mathieu Crosby, Jade Hines, Wilondja Jacob

About Team JenCyber

Jade Hines
Team Lead

Wilondja Jacob
Tech/Research Lead



Mathieu Crosby
Design Lead

Overview

01

JenDore LLC

- *Operates in gaming products and customized retail.*
- *Offers branded items, clothing, gaming accessories, and personalized tumblers.*
- *Success relies on online presence, customer engagement, and digital marketing.*

02

Evolving Retail Industry

- *Retail includes various business models like direct-to-consumer brands, online platforms, and brick-and-mortar stores.*
- *E-commerce has transformed the industry, enabling small businesses to compete in niche markets.*

03

Cybersecurity Risks

- *Small businesses face phishing, fraud, and data breaches.*
- *Weak defenses make them prime hacker targets.*

04

Need For Security

- *Cyber threats impact trust and operations.*
- *Strong Securities ensures business growth.*

Threats Associated With Retail

Small e-commerce businesses like JenDore LLC face cybersecurity risks that threaten operations, customer trust, and finances. Awareness is key to implementing strong security measures.

Cybersecurity Risks in Retail E-Commerce

Small businesses like JenDore LLC face cyber threats that impact operations, customer trust, and finances.

Major Threats

- **Phishing & BEC Attacks** – Fake emails trick employees into sharing data or transferring funds ($2.9B lost in 2023).
- **Ransomware** – Hackers lock data and demand payment (74% increase in losses in 2023).
- **Data Breaches** – Stolen customer credentials lead to fraud and reputational damage.
- **Supply Chain Risks** – Vendor cyberattacks can disrupt operations.
- **Bot Attacks** – AI-driven bots steal data and commit fraud (560K+ daily in 2024).

Protection Measures

Employee training, strong security policies, audits, and expert support help safeguard JenDore LLC.

JenDore Specific with Retail

01 Phishing / BEC

Pretending to be a customer or JenDore to a customer
Fixed with Filtering
Employee Education

02 Data Breaches

Possible attack for customer data
Encrypting Data
Firewalls/Intrusion Detection Systems

03 Ransomware

Locking up inventory data or custom order data
Having back ups

04 Bot Attacks

Effects social media plus website
Having other places to direct people to


Company Overview & Social Presence

Description

JenDore LLC is a woman-owned custom retail startup offering gaming gear, handmade products, and personalized gifts primarily through digital platforms.

History

Founded by Jena Green in Portsmouth, Virginia, JenDore began as a creative outlet and grew into a full-time business built on customization and customer loyalty.

Social Media Audit

Strong visual brand. Risks include impersonation, account hijacking, phishing links.
Recommendations: MFA, strong passwords, content moderation tools.

Company Name: JenDore LLC
🌐 Website: www.jendore.com
📱 Instagram: @jendore.llc | Facebook: JenDore LLC | TikTok: @jendorellc | Pinterest: JenDoreStore | BlueSky: @jendorestore.bsky.social | Twitter: @JenDoreStore | Twitch: JenDore

Social Media Audit

Main Website

Shopping + Doordash
Links to other Social Medias

FaceBook

Gives phone number and email
Posts about pop up times

Instagram

Business chat system
Links to Threads, Website and TikTok

TikTok

For international Buyers
Best for updating stock

Twitter

Has not been updated since 11/24
Links to Mercari

Pinterest

Links to Website and Instagram
Links to Poshmark store

V. Risk Assessment

1. Multi-Factor Authentication (MFA)

- **Status:** Partially implemented
- **Recommendation:** Enable MFA across all admin, email, and payment accounts

2. Data Backup

- **Status:** Partially implemented
- **Recommendation:** Set up automated, encrypted weekly backups

3. Antivirus Software

- **Status:** Mostly Implemented
- **Recommendation:** Configure for automatic scans and updates

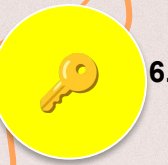
4. Software Updates

- **Status:** Mostly Implemented
- **Recommendation:** Enable auto-updates for OS, software, plugins

5. Phishing Awareness Training

- **Status:** Not Implemented
- **Recommendation:** Quarterly 15-min training sessions

V. Risk Assessment (cont'd)



6. Password Management

- **Status:** Basic passwords
- **Recommendation:** Use a password manager + strong policies

7. Incident Response Plan (IRP)

- **Status:** Not Implemented
- **Recommendation:** Create 1-page IRP with detection, containment, recovery steps

8. Data Encryption

- **Status:** Partially Implemented
- **Recommendation:** Encrypt customer records and backups

9. Vendor Risk Management

- **Status:** Partially Implemented
- **Recommendation:** Use vendor security checklist (MFA, HTTPS, breach history)

10. Social Media Security

- **Status:** Not Implemented
- **Recommendation:** Enable MFA, restrict access, monitor for impersonation

VI. Assets, Risks, and Controls (NIST Framework)

Assets

- E-commerce site (jendore.com)
- Customer & payment data
- Business email & admin accounts
- Social media platforms
- Employee laptops & mobile devices

Risks

- Phishing & email compromise
- Malware/ransomware
- Vendor platform / 3rd party vulnerabilities
- Credential theft
- Social media hijacking

VII. Specific Questions (Client)

1. How do I implement basic cyber risk management practices?

- Identify key assets & risks
- Enable MFA, automate backups, update systems
- Train staff on safe practices

2. How do I create a cybersecurity incident response plan (IRP)?

- Define incident types, roles, and steps
- Include contacts for IT help and law enforcement
- Keep it printed and test it annually

VII. Specific Questions (cont'd)

3. How do I respond to cyberattacks & who do I report to?

- **Respond:** Isolate systems, change credentials, notify partners
- **Report to:**
  - FBI IC3: www.ic3.gov
  - CISA: www.cisa.gov/report
  - Local law enforcement (for data theft or fraud)

4. How do I implement cybersecurity best practices?

- Use secure platforms (HTTPS, reputable vendors)
- Enable MFA everywhere
- Train quarterly
- Regular risk assessments & software updates

Overall Conclusion + SWOT Analysis

Strengths

- Strong online presence
- Responsive brand

Weaknesses

- No formal cybersecurity policy

Opportunities: Use free resources (NIST, CISA, FTC), build customer trust

Threats: Phishing, social engineering, platform attacks

🎯 *Best Bang for Their Dollar: Enable MFA (free) Create simple IRP, Regular backups, Educate yourself about phishing attacks, Use secure e-commerce platforms*

Future Action Plan

🔹 Cyber Hygiene Training:

- 15-min individual training each quarter
- Topics: phishing, password safety, scams

🔹 Incident Response Plan (IRP):

Contact:

- FBI IC3: https://www.ic3.gov
- CISA: https://www.cisa.gov/report
- Local law enforcement for major attacks
- Save emergency contacts offline

✅ Next Steps for JenDore:

- Review & approve IRP
- Implement top 5 action items
- Evaluate Changes with https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset

Resources

Cybersecurity for Small Businesses: Why, What, How

WHY: Growing threats to small businesses (FBI IC3 Report 2023 highlights ransomware, phishing, BEC as major concerns).

WHAT: Key Resources

- **FBI IC3 Report 2023**: Trends and threat insights.
- **CISA Resources**: Tools, tips, protective measures.
- **NIST Framework**: Tailored cybersecurity guidelines.
- **FTC Small Business Guide**: Data security best practices.
- **Valor Digital Security Checklist**: Actionable assessment checklist.

HOW: Implementation Steps

- Regularly review FBI IC3 insights for current threats.
- Apply CISA tools (firewalls, multi-factor authentication).
- Adopt NIST guidelines tailored to your business.
- Follow FTC's recommendations on privacy and security.
- Complete Valor's Security Checklist regularly.
- Foster cybersecurity awareness..

Resources & References Cont.

- *FBI IC3 Report 2023*
- *CISA Cyber Resources*
- *NIST Small Business Cybersecurity*
- *FTC Cybersecurity for Small Business*
- *[Valor Digital Security Checklist (Clinic Resource)]*

Contact Team JenCyber

Jade Hines: *jhine012@odu.edu*

Wilondja Jacob: *wjaco005@odu.edu*

Mathieu Crosby: *mcros016@odu.edu*