Old Dominion University

CYSE 494 Entrepreneurship in Cybersecurity

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Business Plan

Business Name: The Phishing Spear

Email: Jcagl002@odu.edu

Jacob Cagle

**Table of Contents**

Cover Page…………………………………………………………………..……………………………1

Table of Contents……………………………………………………………..…………………………..2

Executive Summary……………………………………………………….….…………………………..3

Business Description……………………………………………………….……………….……………4

Organization and Management………………………………………………..………………………..5

Business Goals……………………………………………………………………….…………………..6

Products or Service…………………………………………………………….………………………...7

Market/Industry Analysis………………………………………………………………………………...8

Marketing and Sales Strategy…………………………………………………………………………..9

Funding Request………………………………………………………………………………………...10

Appendix………………………………………………………………………………………………….11

**Executive Summary**

Business Name: The Phishing Spear

Mission Statement: Providing companies with an adaptive and ever-learning approach that will make cyberspace a safer place.

Vision Statement: To become one of the global leaders in providing cybersecurity support to businesses of all sizes.

Location: Norfolk, Virginia

Products/Services: AI-based anti-phishing cybersecurity platform, browser extension, provides real-time threat reports/analysis, incident report dashboard.

The business that I will be presenting in this plan is based around cybersecurity and the protection of small and large businesses alike. The business name at this stage of planning is called The Phishing Spear. The Phishing Spear is an AI-based anti-phishing cybersecurity company. Our goal is to protect companies from phishing attacks as phishing attacks are one of the leading cybersecurity threats.

**Business Description**

The Phishing Spear AI is an Artificial Intelligence based phishing platform that protects companies from attempted phishing attacks. This AI-based platform is an AI model that will learn overtime and continuously get better at mitigating phishing attacks. The Phishing Spear AI will be a subscription as a service, which will require companies to pay either at a monthly or yearly rate to gain access to our anti phishing software.

Among cyberspace, phishing attacks remain as one of the most common cyber attacks that plague companies by way of human error. The weakest link when it comes to cybersecurity within companies is the ground level employee. All it takes is one employee to click on a link or make a mistake, and all of the information and systems within a company is compromised. With the use of The Phishing Spear, companies can use our tools to mitigate this risk before it ever happens. The Phishing Spear uses its AI-driven model to detect phishing attempts before they trap an employee. Our company uses our machine learning models in combination with our analytics to constantly improve on the accuracy of our detection. Our platform uses our proprietary and exclusive algorithms to accurately evaluate emails and the internet to decipher between real and fake forms of communication.

The Phishing Spear will be designed for growth and user friendly integration. This anti-phishing software appeals to both small start-up companies and large corporations, due to our ease of integration into already existing systems. Our software will seamlessly integrate into already existing email groups and IT environments. With the use of our response dashboard companies can get detailed information on the analysis of their IT environments to analyze the extent of their threat. This will help companies inform their employees and possibly take actionable steps to train their employees on the importance of cyber hygiene.

The Phishing Spear’s target market is all businesses, with a focus on small businesses. We want to cater to small businesses and give them the opportunity to secure their systems while staying within their budget. We can afford to do this because of our subscription as a service. Small businesses would have the opportunity to pay monthly or pay yearly at a cheaper price per month on average. This would give companies the flexibility to buy in at an affordable rate.

We solve both a cybersecurity issue and a cost issue. Like mentioned above, phishing is one of the quickest and easiest ways in which a company can become compromised. We aim to solve this problem and fill a gap in the market by providing an affordable solution to this problem. While our company is catered towards small businesses, businesses of all sizes can take advantage of our service and what we have to offer. Every year small businesses have to shut down based on a cybersecurity breach. We aim to combat this issue by providing an affordable solution. Our unique strength is both ease of integration and affordability making our product the best option for businesses that are looking for a seamless solution to an ongoing problem. We aim to stop the threat before employees click.

**Organization and Management**

This business will be a limited Liability Company (LLC). This best suits this company because it will allow for liability protection while still not levying heavy regulations upon our company. Through this LLC we can still attract potential investors to help fund the startup of our company. Establishing our company as an LLC will also help us in terms of scalability in the future. In terms of positioning/ chain of command within our company, I will recruit a combination of inexperienced and experienced individuals in technology fields. I will tend to recruit folks that have a background/educational experiences in cybersecurity, computer science, and information technology fields. Having a combination of inexperience and experience will both give our company a sense of direction and new/fresh ideas. However, our company could have potential difficulty finding those starting personnel. As the owner I have a vision, but I need the people in which to communicate the vision to. I could also have difficulty finding an experienced research and development team. Finding these experienced personnel to pitch my business to could prove to be difficult, especially considering this idea as a more ambitious business.

General Structure:

Myself, CEO & Founder: I will establish my vision as a basis for the company and a starting point.

Person A, CTO: Experienced individual in preferable a computer science related field.

Person B, Chief Marketing Officer: Experienced individual with a past experience in helping companies market in targeted audiences.

Person C, Chief Financial Officer: Experienced individual with a past experience in helping companies establish a foundation in financial planning and developing reactions with investors (very critical early on).

**Business Goals**

The Phishing Spear aims to achieve both short and long term goals that are both impactful to growth and measurable. In these goals I will focus on the acquisition of customers, development of our product, and leadership among personnel. Our goals will be aimed at innovation at every step to make our company relevant and effective for our customers.

Short Term Goals (Within 24-months):

* Develop product and launch a training product
* Establish connections with at least 10 different companies in various sectors
* Acquire over 50 small paying businesses
* Ensure that our internal environment is exceptional within our workforce (measured by internal survey)
* Attend national cybersecurity conferences to increase brand exposure
* File a patent on AI algorithms

Long Term Goals (After 24-months):

* Reach a company value of over $2 Million dollars year over year
* Expand into other markets overseas
* Expand on features that appeal to larger corporations
* File a patent on a in-house AI model
* Build a nationally recognized incident response team within our platform

These goals outline some of the steps that our company will take in the beginning to establish ourselves as a reliable company for smaller companies to trust. This will allow us to reinvest in ourselves and expand on the ideas that we already have. We look to expand to larger markets in the future (asia/european markets).

The short term goals can prove to be difficult if we have problems developing our research and development team. We also have the potential to run into problems gathering investors and acquiring small paying businesses. We could also run into problems expanding our business overseas. There are many difficulties that could arise when running this business, but these can be overcome by taking actionable steps with operational risk management.

**Product/Services**

Like mentioned above, The Phishing Spear AI offers a variety of cybersecurity tools to help companies defend against phishing attacks. These tools are centered around threat detection and analysis.

Services/Tools:

The Phishing Spear AI detection model: This machine learning AI based model analyzes emails/messages and content within IT environments. Some of those examples can cover mitigating attacks by way of malicious URLs, malicious attachments, and certain patterns used by bad actors.

Browser Extension: This will allow our software to act in real time and mitigate any attack on a potential employee.

Analytical Dashboard: Our dashboard will give companies an overview of the threat that their company may be under. From there they can take actionable steps to mitigate any further occurrence of phishing.

Environmental Toolkits: These training environments can be used to further our advanced AI algorithm to increase the probability of detecting phishing.

Our detection model can scan emails, online activity, and information form submissions. When a threat is detected our system will send a message to the user and the hosts/representatives for that specific company. The IT representative/designated individual will see an exhaustive report of the overall health of the IT environment. Through our Environmental toolkits we will have the ability to scale our model in low risk training environments.

Structure of Pricing (Sale/Production):

* Monthly Subscription: $49.99/user for smaller businesses (scalable based on size)
* Yearly Subscriptions: $360/user for smaller businesses (scalable based on size)

We will also offer custom pricing based on different company needs. Going back to our vision and goals, we want to be the premier company in protecting small businesses. Even if that means catering to their company and changing how we structure our pricing.

* Our startup 24-month startup cost would be around $500,000

Trademark/Patent: This company plans on securing a patent for the algorithm that we use to detect phishing attacks. Once we build a basic product during the startup phase, we will also patent our design for our dashboard. We also plan on trademarking the name of the business and any design for the marketing.

**Market/Industry Analysis**

The Phishing Spear will be operating in a market that grows exponentially year over year. It has surged for many years, with one being the fact that cybercrime is also surging. Businesses all over the world are in need of cyber security, and our company can fill that gap and capitalize on some of the market.

The global cybersecurity market is valued at around $200 Billion and is estimated to reach a market of over $550 Billion by 2033. The phishing protection market in specific is marketed at around $2 Billion in 2023 with an estimated growth of around $4 Billion by 2028. This is very promising for our company and offers room for newer companies to take some market share.

Targeted Customers:

* Small Businesses (20-200 employees) with limited cybersecurity resources
* Sectors such as healthcare, finance, education, government (military, etc.)
* Organizations that need support in mitigating phishing attacks in general

Competitors: SentinelOne and Sophos

* SentinelOne has an AI-driven platform similar to The Phishing Spear. They achieve a 100% detection rate and maintain minimal detection delays according to their website. They specialize in threat detection which would be a big competitor to us. Similar to how I want to run my company, their platform has only gotten better with their use of AI.
* Sophos is a reliable choice for businesses and individuals as they provide malware protection as they focus on endpoint protection. Their antivirus software does well when it comes to threat detection. Some of their major features include antivirus software, remote management, and protection against a variety of cybersecurity threats.

Business Scalability:

Through my analysis of the market involving cybersecurity I think The Phishing Spear has room to grow. Just in the phishing market alone, the market is doubling from $2 billion to $4billion. This growth both points to a need in protection and tells us that there is room for new companies to grow in this market. Due to our AI model based phishing software, we are built for scalability from the beginning. Similarly to SentinelOne, The Phishing Spear AI model will continue to get more accurate as the system learns. If we were to meet our short term goals we would be well within a million dollar company with potential to reach over $10 million dollars.

**Marketing and Sales Strategy**

We aim to rely on a market strategy that focuses on both inbound and outbound market strategies. This can look like things that we create from inside of our company, and also reach out to consumers through the use of more traditional marketing like TV. Our target audience will be cybersecurity consultants and business owners to help us seek opportunities to expand. These business owners will hopefully be looking for an integration friendly anti-phishing tool like our company which will help us expand.

Marketing Strategy:

Inbound marketing

* Content marketing: publishing case studies and statistics on the importance of The Phishing Spear and what it can protect. Showcasing the threat landscape and how The Phishing Spear can protect companies.
* Campaigning: Showcasing what The Phishing Spear can do in real time and providing demos and free trials for potential customers.

Outbound marketing

* Social Media Ads: Use apps that are high in traffic that target smaller businesses
* Conferences: Attend big cyber conferences throughout the year to expose our brand to potential investors and business owners

Like mentioned above, we would create demo builds in which we could showcase our product to business owners. Our sales team guided by our Chief Financial Officer would target businesses via email, follow-ups from conferences, etc. As for distribution, we would have a website that would give access to buy our product (subscription service). We would also allow this service to have availability on app stores through storefronts like Microsoft and Google. Through this we would provide seamless integration with our website extension.

**Funding Request**

Our funding request would be for a total of $500,000 dollars to cover the cost of our first 24 months. This would cover the cost for the development of the product, marketing campaigns (outlined above), and getting the patents listed above. This initial funding would allow us to establish a strong market presence within the anti-phishing market fairly quickly and look to establish ourselves with small business partners.

Funding Allocation

Product Development:

* Roughly $200,000 for software development, developing our cloud infrastructure, and creating the UI

Marketing Efforts:

* Roughly $100,000 to fund our marketing and Sales strategy

Personnel Acquisition:

* $150,000 to hire personnel like engineers that will build out our program, marketing team, various project managers

Legal team and Intellectual property:

* $50,000 for different patents, trademarks, and legal representation

Operations/Infrastructure:

* $50,000 for day to day operations and extra/unaccounted for expenses that arise

**Appendix**

Logo concept:



Slogan used throughout marketing: “stop the risk before you click”

**Works Cited**

Team, B. (2025, April 4). *What are the 9 startup costs for a cyber security business?* Business Plan Templates. https://businessplan-templates.com/blogs/startup-costs/cyber-security

Allied Market Research, https://www.alliedmarketresearch.com/. (n.d.). *Cyber Security Market Size, Share, Competitive Landscape and Trend Analysis Report, by component, by deployment model, by enterprise size, by Industry vertical : Global Opportunity Analysis and Industry Forecast, 2024-2033*. Allied Market Research. https://www.alliedmarketresearch.com/cyber-security-market

*Phishing Protection Market Size & Trends, Growth Analysis, Industry forecast*. (n.d.). MarketsandMarkets. <https://www.marketsandmarkets.com/Market-Reports/phishing-protection-market-103391093.html>

SentinelOne. (2024, December 11). *SentinelOne Sets the Standard with 100% Detection and 88% Fewer Alerts than Median Across All Vendors Evaluated in the 2024 MITRE ATT&CK® Evaluations: Enterprise*. <https://www.sentinelone.com/press/sentinelone-sets-the-standard-with-100-detection-and-88-fewer-alerts-than-median-across-all-vendors-evaluated-in-the-2024-mitre-attck-evaluations-enterprise/>

*Sophos Antivirus Review*. (n.d.). Cybernews. <https://cybernews.com/best-antivirus-software/sophos-antivirus-review/>

OpenAI. (2025). *ChatGPT* (Mar 14 version) [Large language model]. <https://chat.openai.com/chat>

*Note.* Image generated with the prompt “logo including a blue fish with a spear including the “The Phishing Spear” title” by OpenAI, *ChatGPT*, 2025 (https://chat.openai.com/chat).