

Define CS, fit into CC	1. CUSTOMER SEGMENT(S) CS Who is your customer? web phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy website on the Internet.	6. CUSTOMER CONSTRAINTS Hishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme.	5. AVAILABLE SOLUTIONS AS Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly. Firewall protection prevents access to malicious files by blocking the attacks	Explore AS, differentiate
	2. JOBS-TO-BE-DONE / PROBLEMS J&P Which jobs-to-be-done (or problems) do you address for your customers? Email addresses are easy to obtain, and emails are virtually free to send. With little effort and cost, attackers can quickly gain access to valuable data.	9. PROBLEM ROOT CAUSE PC More specifically, a lack of employee training focusing on issues such as phishing and ransomware is the main reason for these attacks being so successful	7. BEHAVIOUR BE It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message	
	3. TRIGGERS TR What triggers customers to act? Spear phishing. There are two other, more sophisticated, types of phishing involving email. ... Whaling. Whaling attacks are even more targeted, taking aim at senior executives. ... Smishing and vishing	10. YOUR SOLUTION SL If you are working on an existing business, write down your current solution first, fill in the canvas, and check how much it fits reality. Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer.	8. CHANNELS of BEHAVIOUR CH 8.1 ONLINE What kind of actions do customers take online? Extract online channels from #7 First, a hacker may gain valuable access to a single account through a successful phishing attempt. Second, if an employee is using the same password for multiple company accounts, then the hacker has now gained access to a great deal of confidential company	
	4. EMOTIONS: BEFORE / AFTER EM Greed. Here's an example of a phishing email your employees might receive that uses greed to try to get them to click a link. ... Curiosity. ... Urgency			