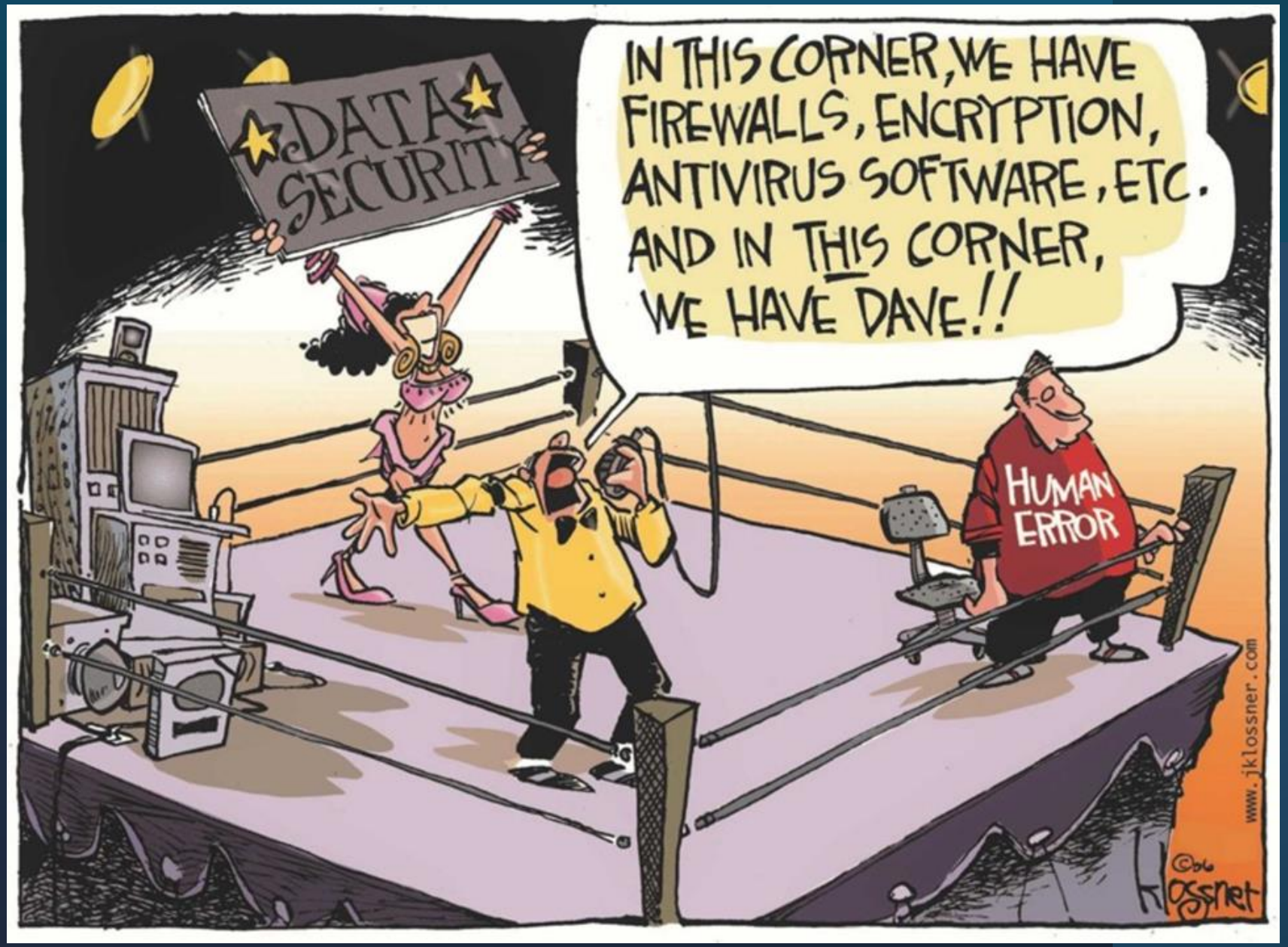
Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors

Presented by
Tommy Pollock

TIDEWATER COMMUNITY COLLEGE
CENTER FOR WORKFORCE SOLUTIONS
50 YEARS
Go Further!

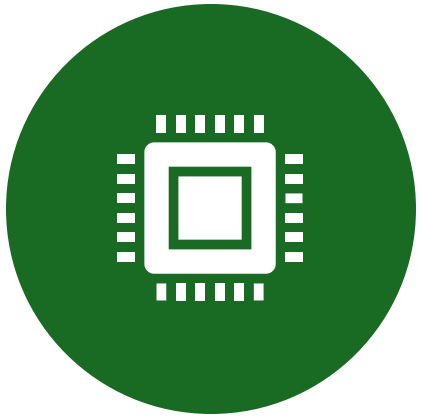
http://CyLab.nova.edu/

NSU Florida
College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©'06
Klossner

Rationale for the Research

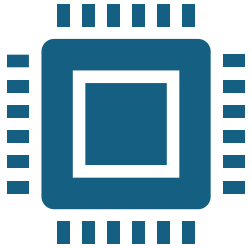
PHISHING CONTINUES TO BE AN INVASIVE THREAT TO COMPUTER AND MOBILE DEVICE USERS (MCELWEE ET AL., 2018).



DECEPTIVE SEARCH ENGINE RESULTS POSE A PROBLEM BECAUSE CYBERCRIMINALS OFTEN MANIPULATE THE RESULTS ALGORITHMS THROUGH SEARCH POISONING TECHNIQUES, WHICH PROMOTE MALICIOUS LINKS TO THE FIRST PAGE OF THE SEARCH ENGINE RESULTS (JOHN ET AL., 2011; LEONTIADIS ET AL., 2014).

USERS OF MOBILE PHONES, IN PARTICULAR, ARE MORE VULNERABLE TO PHISHING ATTACKS THAN THOSE WHO USE PERSONAL COMPUTERS (PCS) DUE TO POOR FRAUDULENT WEBSITE DETECTION OF SOME MOBILE BROWSERS ALONG WITH THE LIMITATION OF THE SMALLER SCREEN (MAVROEIDIS & NICHO, 2017; TSALIS ET AL., 2015; VIRVILIS ET AL., 2014).

Why This Research is Important



In today's digital age, cyber threats are evolving rapidly, and phishing attacks remain one of the most prevalent and dangerous forms of cybercrime. One particularly insidious tactic involves the use of Cyrillic alphabetic letters to deceive unsuspecting users. Here's what you need to know to stay safe:

Fake URLs: A URL like "**www.example.com"** could be spoofed as "**www.exɑmple.com**" using the Cyrillic "а". This fake URL might lead to a phishing site designed to steal your credentials.

Email Addresses: An email from "**support@company.com**" could be faked as "**support@compɑny.com**", making it difficult to spot the phishing attempt.

Screen Size Make a Difference

MOBILE USERS FACE A HEIGHTENED RISK OF FALLING VICTIM TO PHISHING ATTACKS COMPARED TO DESKTOP USERS. THE UNIQUE VULNERABILITIES OF MOBILE DEVICES, COUPLED WITH THE WAYS IN WHICH PEOPLE USE THEM, MAKE THEM ATTRACTIVE TARGETS FOR CYBERCRIMINALS.

THE COMPACT NATURE OF MOBILE DEVICES PLAYS INTO THE HANDS OF ATTACKERS ALLOWING THEM TO PLAY HIDE AND SEEK WITH CRUCIAL DETAILS, LIKE URL OR EMAIL HEADERS. THESE LIMITATIONS, COUPLED WITH USER INCONVENIENCE WHEN INPUTTING ON SMALLER SCREENS AND THE GENERAL HABITS AND PREFERENCES OF MOBILE USERS, SIGNIFICANTLY AMPLIFY THE RISK OF FALLING VICTIM TO A SUCCESSFUL PHISHING ATTACK.

Disadvantages of Smartphones:

Addiction and Distraction: Overuse leading to reduced productivity.

Privacy Concerns: Personal data vulnerabilities and tracking.

Health Issues: Eye strain, sleep disruption, and poor posture from prolonged use.

Cybersecurity Threats: Susceptibility to hacking, phishing, and malware.

Cost: Expensive to purchase and maintain, including data plans.

Social Isolation: Reduced face-to-face interactions and communication.

Short Battery Life: Frequent charging and reliance on power sources.

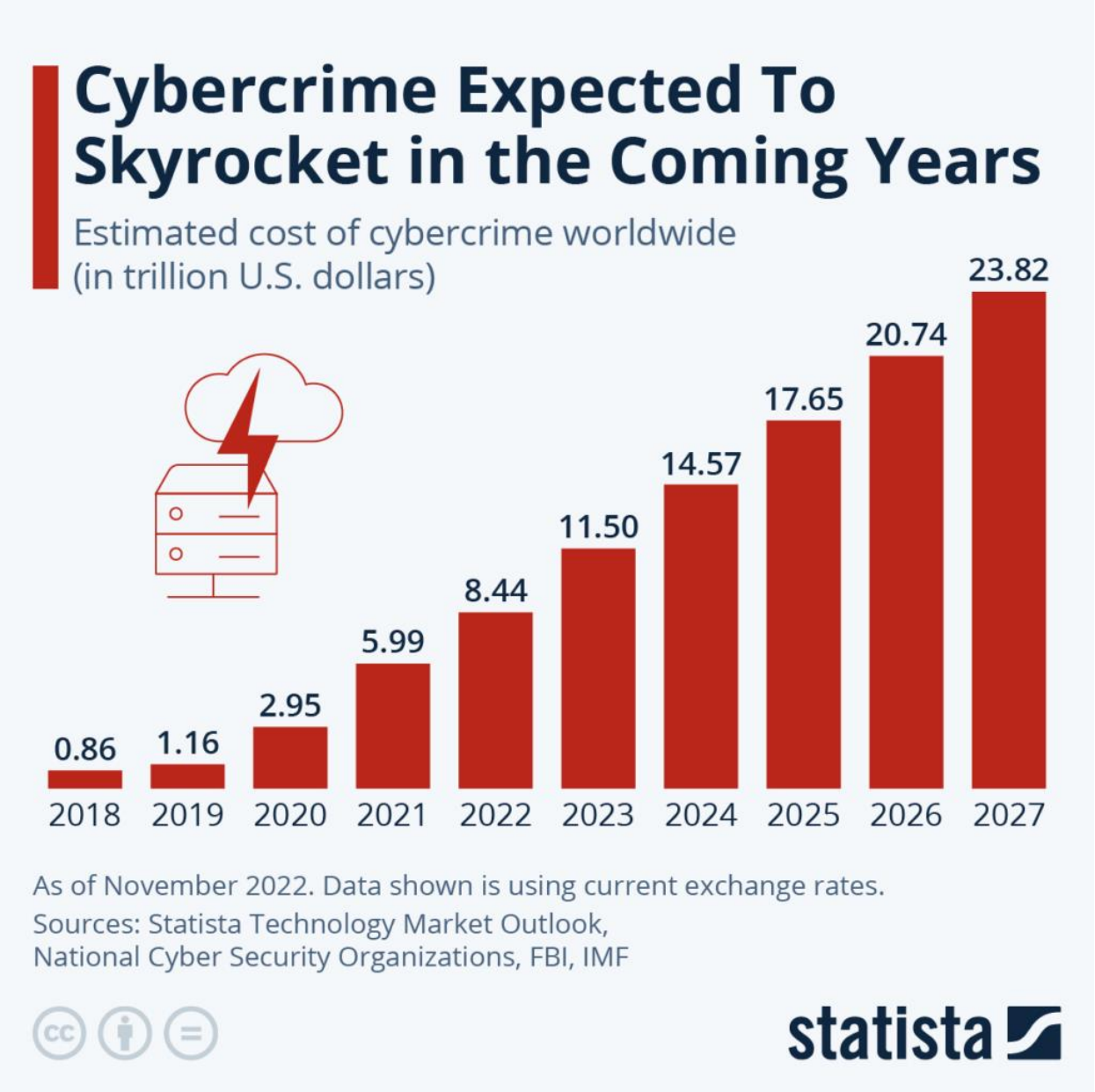
Environmental Impact: Electronic waste and resource consumption during production.

Some Warning Signs of a Phishing Attack

Cyber Attack Vectors

Cyber Attack Targets

Financial Costs of Cybercrime



Why Do Educated Users Fall for Phishing Scams?

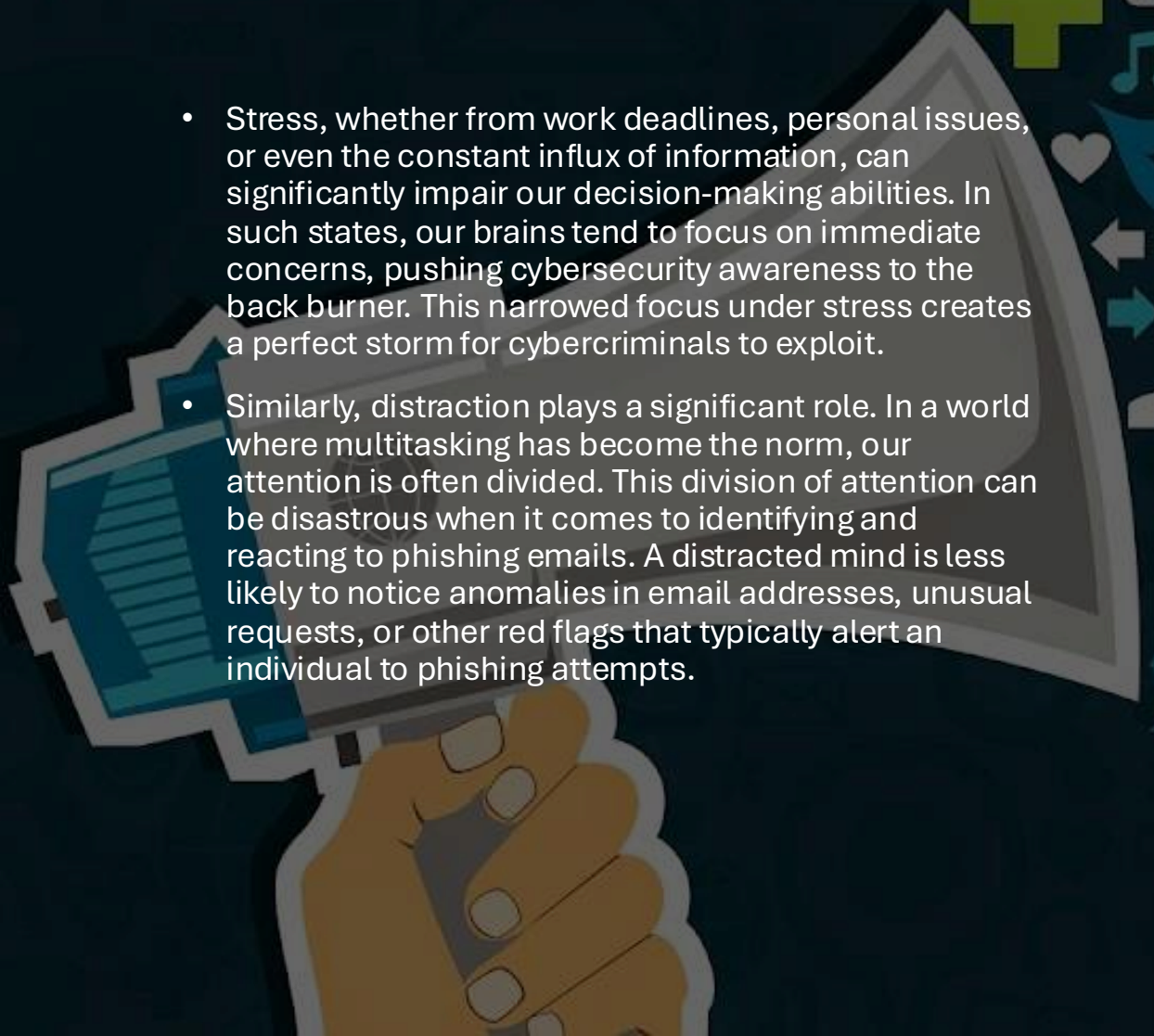
- It’s a perplexing situation: individuals who are knowledgeable about cybersecurity, and who may have even completed rigorous security awareness training, still fall prey to phishing scams. Why does this happen, even to the best of us?
- The answer lies in the unique challenges posed by stress and distraction. Under pressure or when multitasking, our cognitive resources are stretched thin. This diminished capacity can lead to a lapse in judgement, causing even the most cyber-savvy individuals to miss the subtle cues of a phishing attempt.

Phishing Vulnerabilities that are Exploited

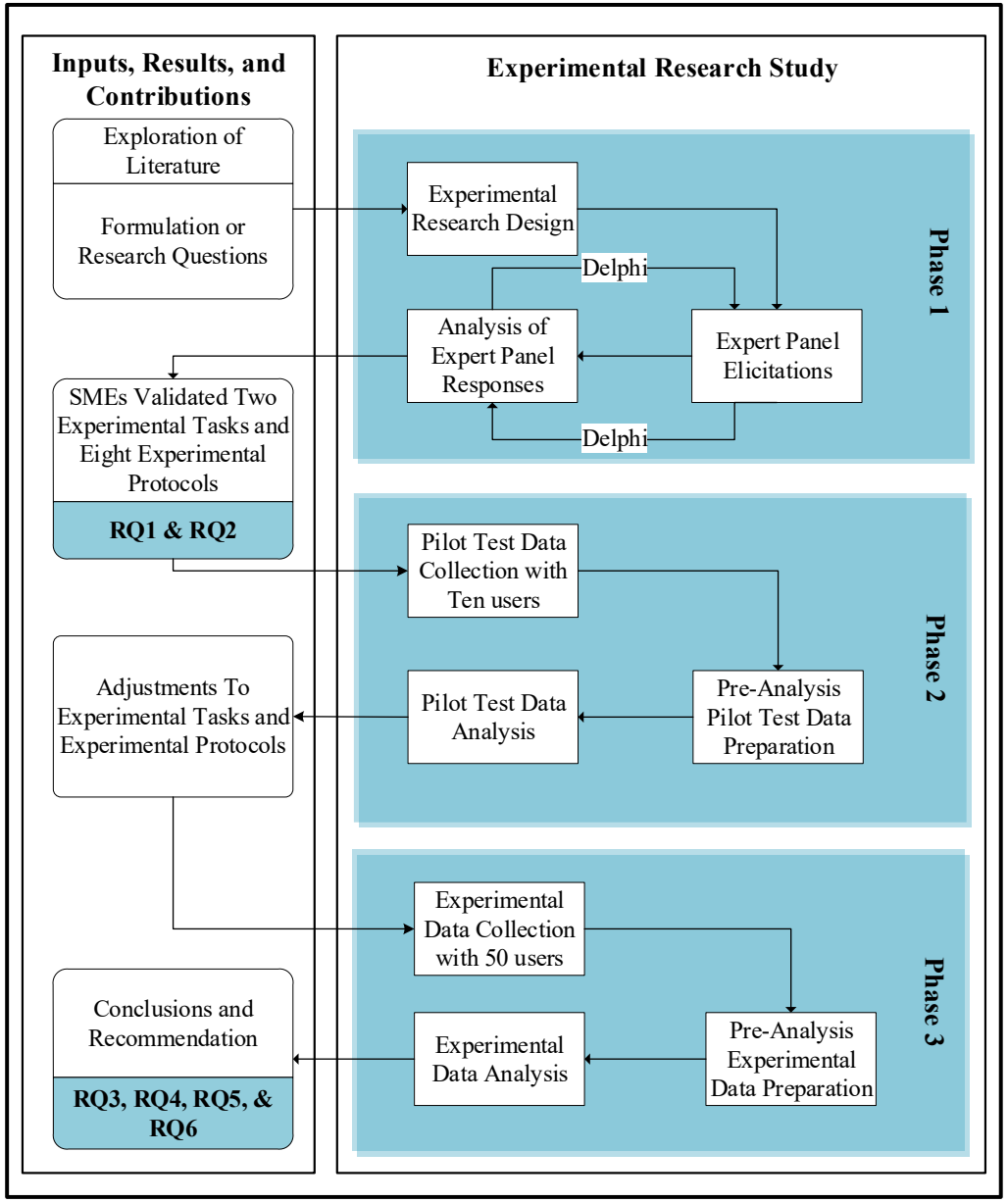
- **Psychological factors** play a significant role in phishing susceptibility as attackers often exploit common cognitive biases and emotional triggersto manipulate users. Key psychological factors include trust and authority, where phishing emails often impersonate authoritative figures or trusted organizations to gain credibility. Fear and urgency are also common tactics, as messages that invoke fear or a sense of urgency can prompt users to act quickly without carefully thinking and evaluating the email's legitimacy. Additionally, greed and curiosity can entice users to interact with such emails by promising financial gain, rewards, or other kind of profit.
- Some other factors that also impact susceptibility to phishing are **behavioral tendencies**. Routine and habit play a key role, as users that are used to clicking on links or opening attachments without scrutiny are more likely to fall for phishing emails. Furthermore, a lack of awareness on phishing techniques and the associated risks makes users more vulnerable.
- **Contextual elements** refer to the situational circumstances that affect a user's likelihood of falling for a phishing email. Time pressure is a significant factor, as users under time constraints may not take the time to thoroughly evaluate the legitimacy of an email. Distraction also plays a key role; multitasking or being in a distracting environment without paying the attention needed can reduce a user's ability to detect phishing cues. On the other hand, the type of device used, such as a mobile phone with a smaller screen, can make it harder to notice signs of phishing. Additionally, the organizational environment, including the culture and security practices of an organization, can influence user susceptibility
- **Demographic factors** refer to the statistical characteristics of a population such as age, gender, and education level that can influence a user's susceptibility to phishing attacks. Research indicates that younger and older individuals may be more vulnerable compared to middle-aged adults. Younger users are more familiar with technology, and this might exhibit overconfidence in their ability to detect phishing, leading to riskier online behaviors. Conversely, older adults might lack the digital familiarity required to recognize phishing attempts, making them the main targets for attackers .Gender differences also play a role; studies have shown that women are generally more cautious and may be less likely to fall for phishing email than men, who might take more risks online. Additionally, users with higher levels of education are typically better at identifying phishing emails due to greater exposure to information about cybersecurity threats.

The Role of Stress and Distraction

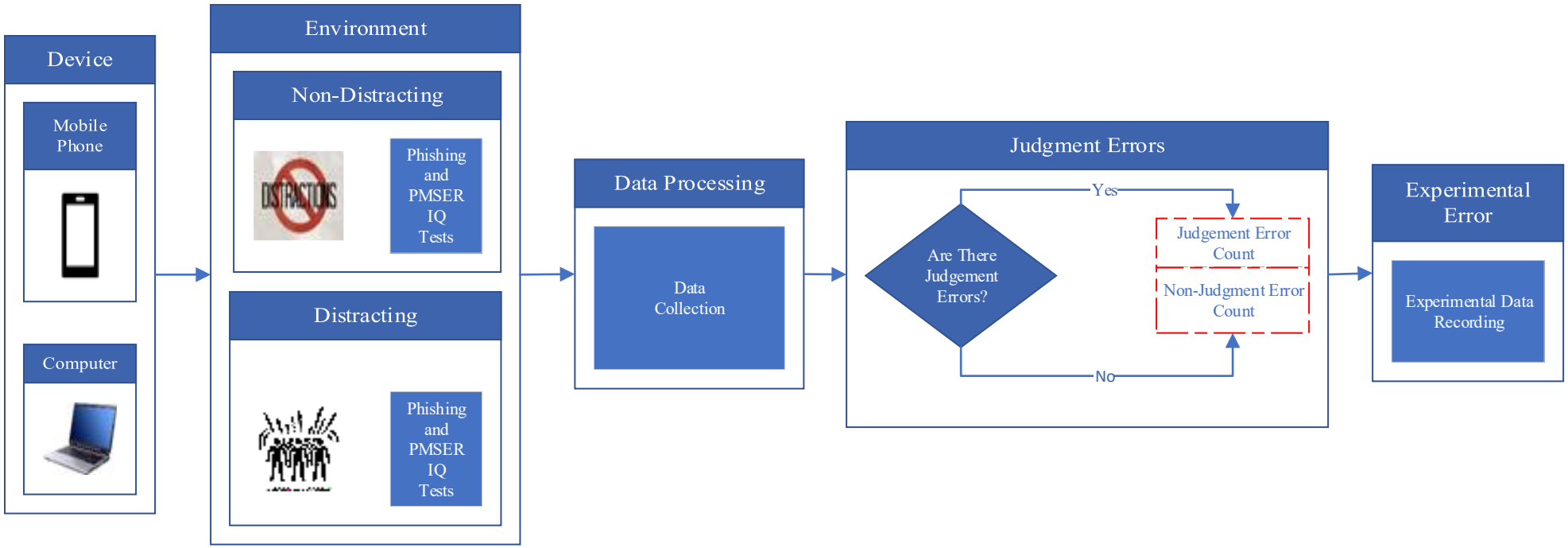
- Stress, whether from work deadlines, personal issues, or even the constant influx of information, can significantly impair our decision-making abilities. In such states, our brains tend to focus on immediate concerns, pushing cybersecurity awareness to the back burner. This narrowed focus under stress creates a perfect storm for cybercriminals to exploit.
- Similarly, distraction plays a significant role. In a world where multitasking has become the norm, our attention is often divided. This division of attention can be disastrous when it comes to identifying and reacting to phishing emails. A distracted mind is less likely to notice anomalies in email addresses, unusual requests, or other red flags that typically alert an individual to phishing attempts.



Methodology Experimental Field Study

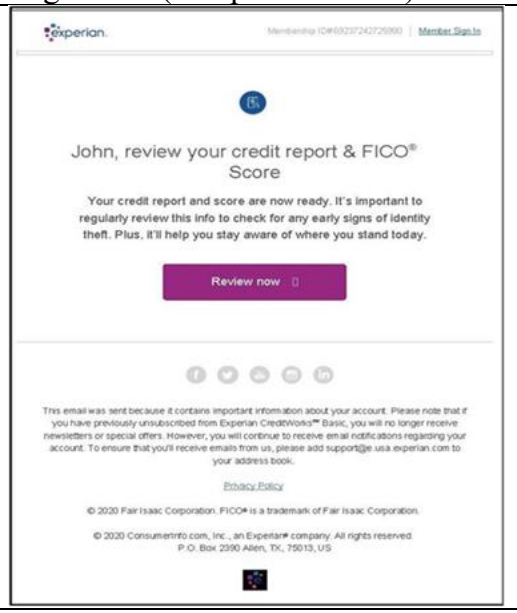


Collection Methodology

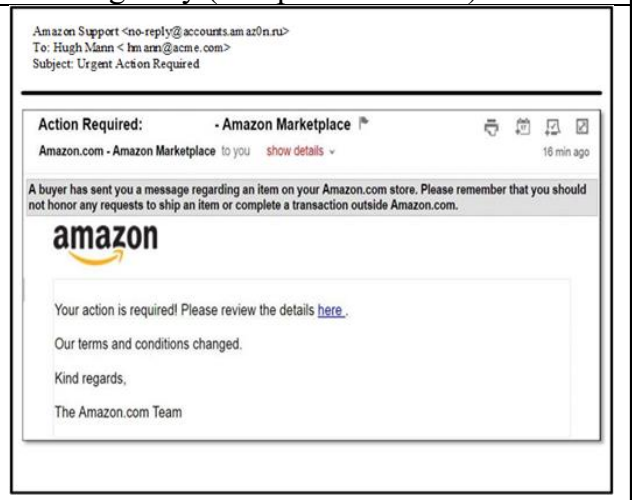


Phishing Email Samples

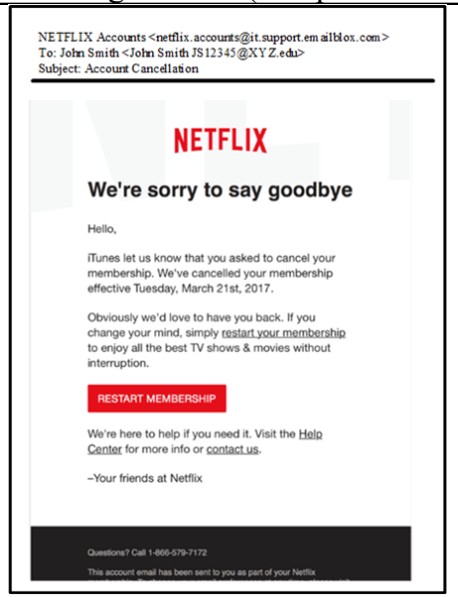
Legitimate (Sample 3 Table 2)



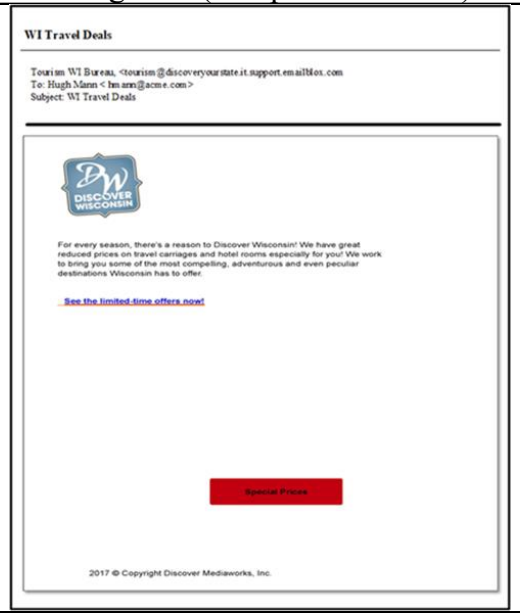
Phishing Easy (Sample 10 Table 2)



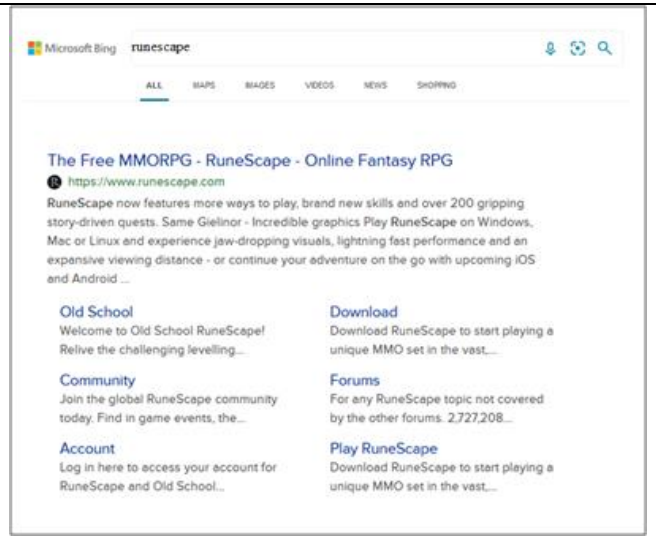
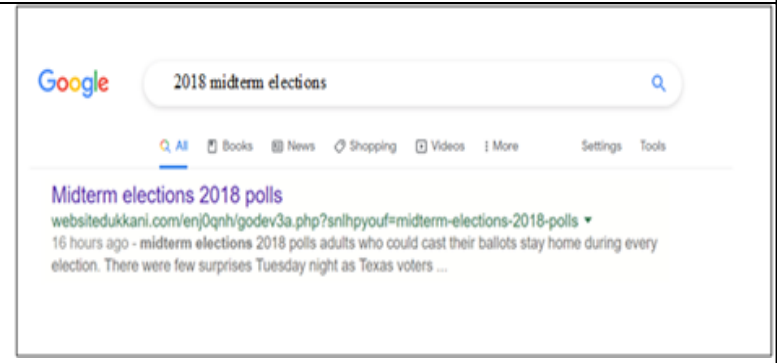
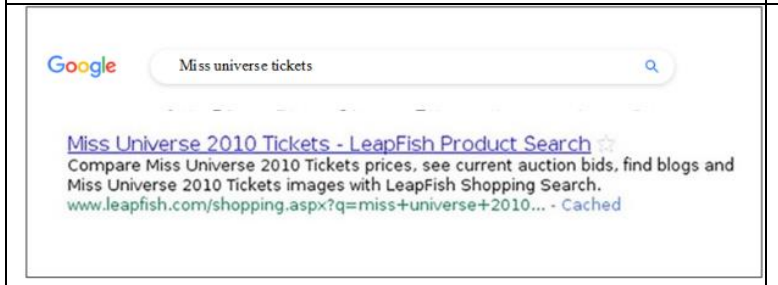
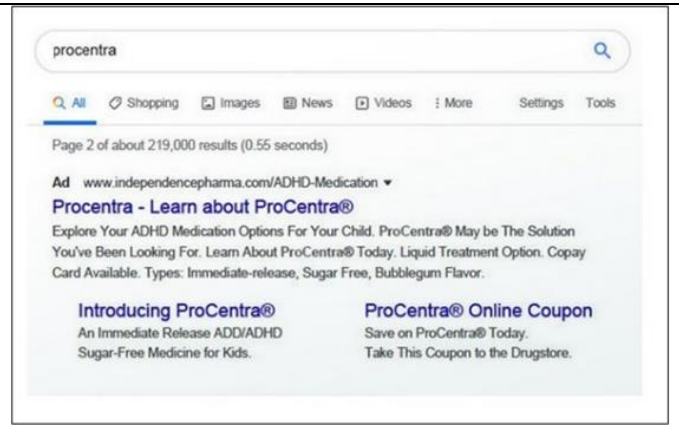
Phishing Medium(Sample 4 Table 2)



Phishing Hard(Sample 11 Table 2)



PMSER Samples

Legitimate (Sample 10 Table 4)	PMSER Easy (Sample 8 Table 4)
	
PMSER Medium (Sample 2 Table 4)	**PMSER Hard (Sample 12 Table 4)**
	

Phishing and PMSER Mini IQ Tests. Phase 1

Social Engineering Attack Type

Phishing

Device	Environment: Distracting	Environment: Non-Distracting
Mobile Phone	Distracted via Mobile Phone • Phishing Hard • Legitimate • Phishing Easy	Not Distracted via Mobile Phone • Legitimate • Phishing Easy • Phishing Medium
Computer	Distracted via Computer • Phishing Easy • Phishing Medium • Phishing Hard	Not Distracted via Computer • Phishing Medium • Phishing Hard • Legitimate

PMSER

Device	Environment: Distracting	Environment: Non-Distracting
Mobile Phone	Distracted via Mobile Phone • Legitimate • PMSER Easy • PMSER Medium	Not Distracted via Mobile Phone • PMSER Easy • PMSER Medium • PMSER Hard
Computer	Distracted via Computer • PMSER Medium • PMSER Hard • Legitimate	Not Distracted via Computer • PMSER Hard • Legitimate • PMSER Easy

Thank You