ANALYSIS OF SQL INJECTION AND PHISHING ATTACKS: TECHNIQUES, IMPACTS, AND MITIGATION STRATEGIES

Christian Jay F. Dimas

IT IAS1 - Information, Assurance, and Security 1

COR JESU COLLEGE, INC.

May 2025

CIEMAVIL S. ALCAIN

ABSTRACT

This research looks at two common types of cyber attacks: SQL injection and phishing. It explains how these attacks work, what methods are used, and how they can harm people and organizations. SQL injection attacks target databases by putting harmful code into input fields, while phishing tricks people into sharing personal or login information. Both can lead to data loss, financial damage, and loss of trust. The paper also talks about ways to prevent and reduce these threats, such as using secure coding practices, educating users, and using security tools. The goal is to help readers understand these attacks and how to protect against them in simple terms.

Keywords: *SQL Injection, Phishing, Cybersecurity, Data Breaches, Mitigation Tecniques*

TABLE OF CONTENTS

INTRODUCTION

Today, we use the internet for many things such as shopping, paying bills, working, or even talking with your friends. This means a lot of important information like personal information is stored online. Cyber attacks are a big problem for people and organizations today. Two common types of attacks are SQL Injection and Phishing (Kaspersky, 2023). The impact SQL Injection and Phishing can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business (Sharadin, 2023).

In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it. In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, you'll thereby install malware in your computer. If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file, except the website is actually a trap used to capture your credentials when you try to log in (Cyber Security Unity, 2025).

SQL injection is a security weakness in web applications that enables an attacker to manipulate the queries sent from an application to its database. This may enable an attacker to access information that they typically cannot obtain. This could encompass information that is owned by other users or any other information that the application is able to reach. In numerous situations, an intruder can alter or remove this information, leading to lasting modifications in the application's content or functionality (Web Security Academy, n.d.).

Understanding the vulnerabilities that lead to SQL injection and phishing attacks is essential for improving cybersecurity. By identifying weak points in systems and user behavior, organizations can take steps to protect sensitive data and reduce the risk of financial and reputational damage. Studying these weaknesses also helps in developing

better tools and strategies to detect and stop attacks before they cause harm (OWASP, 2023).

These are the common research questions or hypotheses of the study:

- What are the most common signs of phishing emails?
- How can companies prevent SQL injection attacks on their websites?
- Why do some people fall for phishing more easily than others?
- How much money is lost each year due to phishing and SQL injection?

By answering these questions, this study aims to analyze the techniques used in SQL injection and phishing attacks, examine their impacts on individuals and organizations, and explore effective strategies to prevent and reduce these cybersecurity threats.

OBJECTIVES OF THE RESEARCH

- Identify common techniques used in SQLi and Phishing attacks.
- Analyze real-world impacts of these attacks
- Explore prevention and mitigation strategies
- Raise awareness about cybersecurity best practices

SQL INJECTION: OVERVIEW AND ANALYSIS

SQL injection (SQLi) is a type of cyber attack where a hacker puts harmful code into a website's input fields, like a search box or login form, to trick the system into giving access to the database. Normally, websites use SQL (Structured Query Language) to talk to databases and manage information like usernames, passwords, and customer data. When a website doesn't properly check or clean the user's input, a hacker can enter SQL commands that the system will run. This can let the hacker see, change, or delete important data, even if they don't have permission. In some cases, they can take full control of the database (OWASP, 2023).

I. TYPES OF SQL INJECTIONS

The most common types of SQL injection attacks include Union-based, Error-based, Blind, and Time-based SQL injections. Each of these methods operates differently and presents unique detection and prevention challenges. A

clear understanding of these types is essential for developing effective defenses against SQL injection threats (OWASP, 2023; Acunetix, 2023).

1. **Union-based SQL injection**

   Is a technique where attackers use the SQL UNION operator to combine the results of two or more SELECT queries into a single result. This allows them to retrieve data from other database tables that they normally wouldn't have access to.

   For example, if a website allows users to search for products using a search box, and that input is not properly checked, a hacker might enter a special query like:

   Copy Edit ' UNION SELECT username, password FROM users --

   If the site is vulnerable, it may display usernames and passwords from the users table instead of normal search results. Union-based attacks are dangerous because they can expose sensitive data, such as login credentials, emails, or financial information, with just a few lines of injected code (PortSwigger, n.d.).

2. **Error-Based SQL Injection**

   Error-based SQL injection is a technique that takes advantage of a database's error messages to gain information about its structure. When a website does not properly handle errors, attackers can insert SQL commands that force the database to generate an error. These error messages may reveal useful details, such as table names, column names, or even data stored within the database.

   For example, if a hacker inputs:

   Copy Edit ' OR 1=1 ORDER BY 100 –

   and the database returns an error like "Unknown column," this tells the attacker that there are fewer than 100 columns. By adjusting the query and

observing the errors, attackers can map out the database and launch further attacks. This method is often used as a starting point to plan more targeted SQL injection techniques (OWASP, 2023).

3. **Blind SQL Injection**

Blind SQL injection is a type of attack used when the web application does not display error messages or output data directly. In this case, the attacker cannot see the results of their injected SQL queries, so they must ask the database true or false questions and observe how the application behaves.

For example, an attacker might enter:

Copy Edit ' AND 1=1 --

If the page loads normally, it suggests the condition is true. Then they might try:

Copy Edit ' AND 1=2 --

If the page behaves differently, it shows the condition is false. By repeating this process and changing the conditions, the attacker can slowly gather information from the database, such as table names, column names, or user data. Blind SQL injection is slower than other methods, but it can still be very effective, especially on websites that hide error messages for security (Acunetix, 2023).

4. **Time-Based SQL Injection**

Time-Based SQL Injection Time-based SQL injection is a type of blind SQL injection where attackers determine whether their injected queries are successful by measuring how long it takes the database to respond. Instead of relying on error messages or visible output, the attacker uses SQL commands that cause a deliberate delay in the

database’s response when a certain condition is true.

For example, an attacker might use:

Copy Edit ' IF(1=1, SLEEP(5), 0) --

If the page takes 5 seconds to load, it means the condition was true. If it loads instantly, the condition is false. By repeating this method with different queries, attackers can slowly extract information such as usernames, passwords, or structure details from the database. Although time-based SQL injection can be slow, it is effective when no data is visibly returned, and all other feedback methods are blocked (PortSwigger, n.d.).

II. REAL-WORLD EXAMPLES

1. Heartland Payment System (2008

In 2008, Heartland Payment Systems suffered a massive data breach affecting over 130 million credit and debit card accounts. Attackers used SQL injection to infiltrate the company's network, installing malware that captured card data as it was processed. This breach remains one of the largest of its kind and underscores the importance of securing payment systems against injection attacks (*Heartland Breach: Inside Look at the Plaintiffs’ Case*, n.d.)

2. Sony Pictures Entertainment (2011)

In June 2011, the hacker group LulzSec exploited a SQL injection vulnerability on Sony Pictures' website to access and leak personal data of over 1 million users. The exposed information included usernames, passwords, and email addresses. The breach was part of a series of attacks on Sony's networks, highlighting significant security lapses (Poulsen, 2011).

III. TOOLS FOR EXPLOITATION

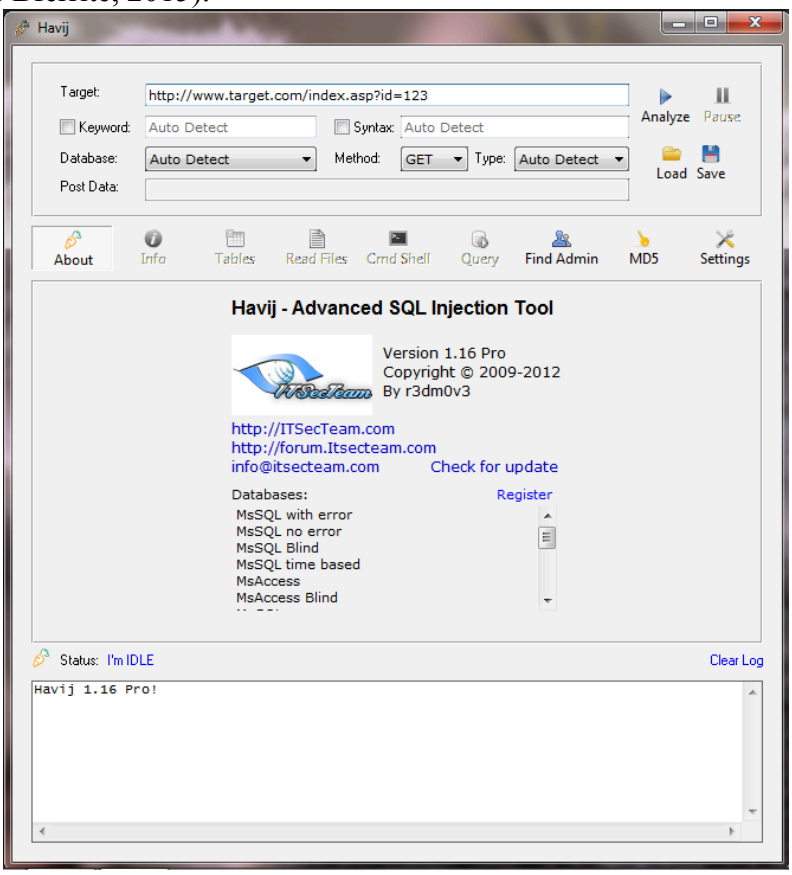
1. SQLMap

Sqlmap is a free tool used in security testing that helps find and use SQL injection problems in websites. It can automatically detect these issues and even take control of the database server. It has a strong detection system and many features for advanced users. With it, you can figure out what kind of database is being used, pull out data, access files on the server, and even run system commands using special connection methods (*Sqlmap: Automatic SQL Injection and Database Takeover Tool*, n.d.).

2. Havij

Havij is an automatic SQL injection tool created by ITSecTeam, a security company from Iran. "Havij" means "carrot" in Persian, which is also shown in the tool's icon. It has an easy-to-use interface, making it simple for users to get data from vulnerable websites. This user-friendly design may have led to more non-technical people using it for attacks, instead of only skilled hackers. Havij was released in 2010. Since then, other tools like sqlmap have come out, but

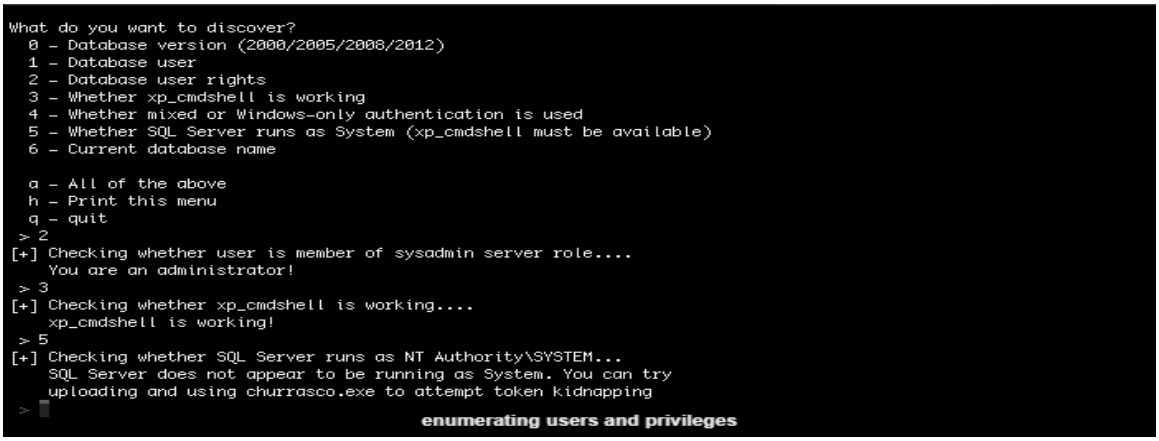
Havij is still being used today by both professional testers and beginner hackers (Bferrite & Bferrite, 2015).



3. SQLNinja

Sqlninja is a tool used to take advantage of SQL injection problems in web applications that use Microsoft SQL Server. The main goal of sqlninja is to take control of the database server through one of these flaws.

It is written in Perl and is included in the Kali Linux system under Applications, Database Assessments. Unlike some other tools, sqlninja does not find SQL injection issues, it only helps exploit them to get remote access on the server (Najera-Gutierrez & Ansari, n.d.).



PHISHING: OVERVIEW AND ANALYSIS

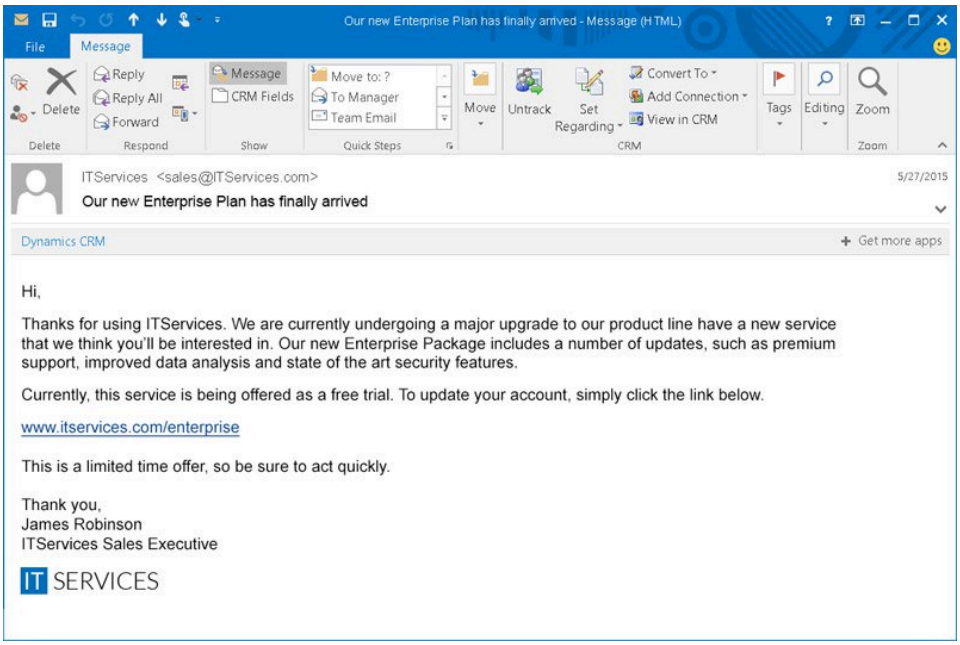
Phishing is a common online scam where attackers try to trick people using emails, text messages, phone calls, or other ways of communication. The goal is to fool the person into doing something the attacker wants—like giving away bank details, login passwords, or other private information. These attacks mainly take advantage of how people think and act, not problems in the computer system. Phishing is a type of social trick. The attackers pretend to be someone you trust, like a company or organization, to mislead you. They might ask you to click on a fake website, download harmful files, or share personal information like your bank or credit card number (ProofPoint US, 2025)

I. TYPES OF PHISHING ATTACKS

Phishing remains one of the most pervasive and damaging forms of cybercrime, leveraging social engineering techniques to trick individuals into divulging sensitive information. While traditional phishing casts a wide net to capture as many victims as possible, modern variants have evolved to become more targeted and sophisticated (Jain & Gupta, 2018). Understanding the various forms these phishing attacks can take is essential for both individuals and organizations in developing effective defenses against them.

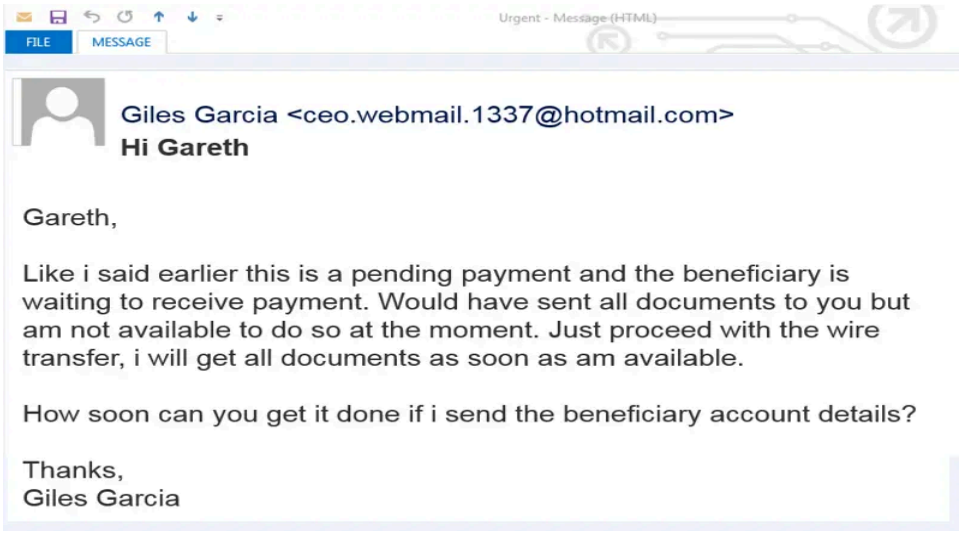
1. Spear Phishing

Spear phishing is a type of phishing that targets specific people or organizations. Unlike regular phishing, which sends fake messages to many people, spear phishing focuses on one person or group and uses personal details to make the message look real. The attacker starts by finding information about the target. They often look at social media, company websites, or news articles to learn about the person's job, interests, and other details. They may even use public tax information. Then, the attacker uses this information to write a message, usually an email that seems to come from someone the person trusts, like a coworker or business partner (ProofPoint US, 2025).



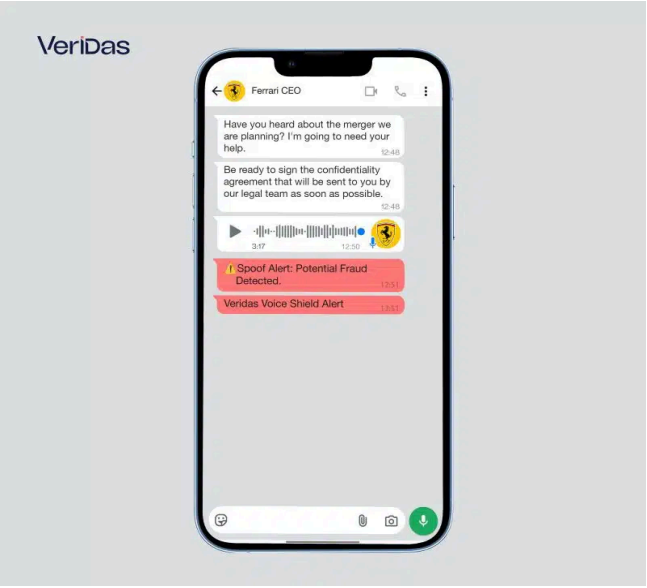
2. Whaling

A whaling attack is a special kind of phishing that targets important people in a company, like the CEO or CFO. The goal is usually to trick them into sending large amounts of money to the attacker or giving away secret company information. The name "whaling" comes from the idea that these attacks go after the “big fish” in a company—people with power and access to valuable information. Because these attacks are very targeted and convincing, they are harder to spot than regular phishing. To help stop whaling attacks, companies should make sure their top managers get training on how to stay safe online and recognize scams (Robinson et al., 2024).



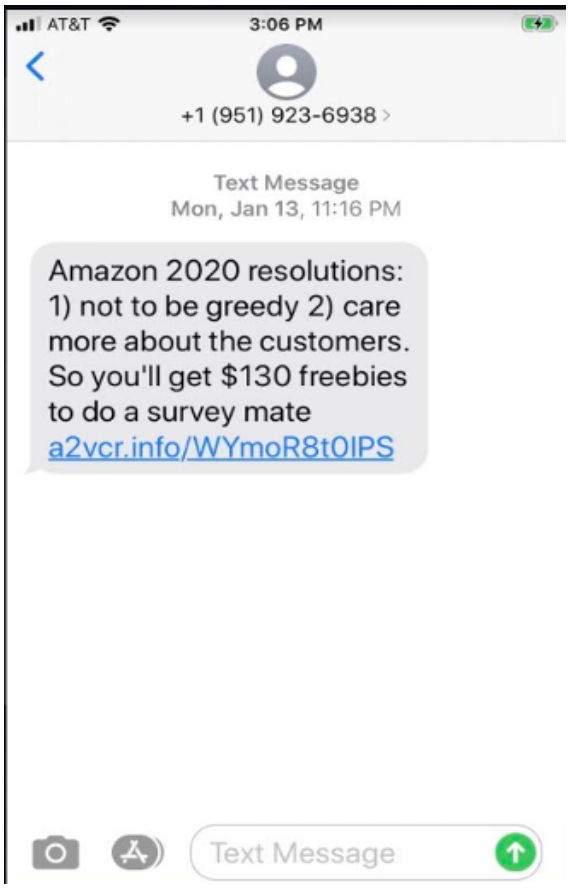
3. Vishing

Vishing, short for voice phishing, is a scam where criminals use phone calls or voice messages to trick people into giving away private information, like passwords, credit card numbers, or bank details. This information is then used for crimes like identity theft or stealing money. In 2022, phishing attacks caused major problems for companies, with the average cost of a data breach being about $4.91 million. In vishing attacks, the scammer often pretends to be someone trustworthy—like a bank worker, a government employee, or a delivery service. They may use phone numbers that look real or use internet phone systems (VoIP) to fake their identity. Sometimes, vishing begins with an email that asks the person to call a number. When the person calls, the scammer tries to trick them into giving out personal details using smart and convincing language (called social engineering). These scams often target older adults, new staff, or people who talk to customers or suppliers on the phone. To stay safe, it's important to be careful, stay informed, and use strong security for email and phone systems (Secure Email Threat Defense Demo, 2025).



4. **Smishing**

Smishing is a type of phishing scam where criminals send fake text messages to trick people into clicking bad links or sharing personal information, like bank details or passwords. The main difference from other phishing attacks is that smishing uses text messages (SMS) or messaging apps instead of emails or phone calls. Scammers like smishing because people are more likely to click on links in texts. For example, studies show that text message links get clicked much more often than links in emails. To hide where their messages come from, scammers might fake phone numbers, use burner phones, or send texts through email software. It's also harder to spot fake links on a phone. On a computer, you can hover over a link to see where it goes but phones don't have that feature. Plus, people are used to getting texts from banks or companies, often with short links, so they're less suspicious (Kosinski, 2025).

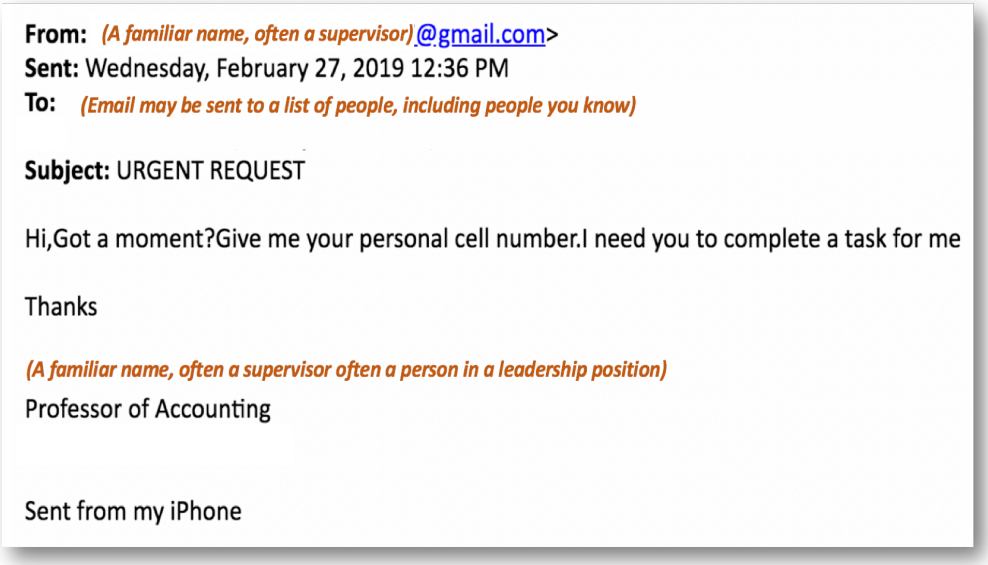


II. PSYCHOLOGICAL TACTICS

Phishing attacks work by tricking people using emotions and mental shortcuts. Scammers try to make people feel scared.

1. Urgency

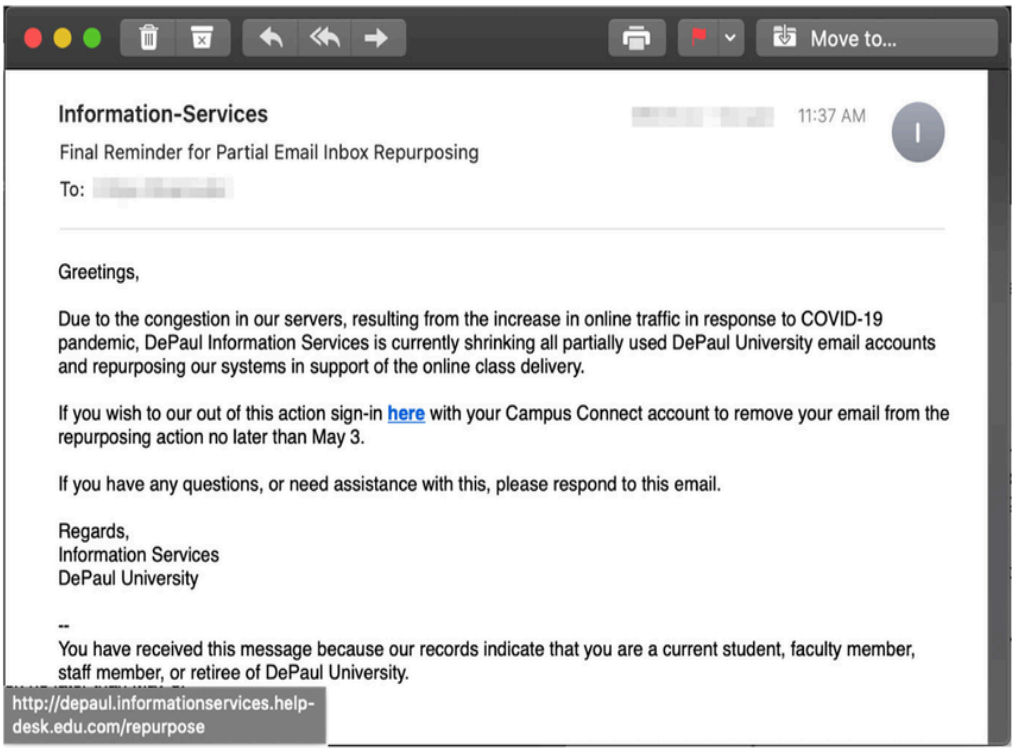
Phishers take advantage of how people like to act quickly when they think something is about to run out or they might lose something. They make people feel like they must hurry, so they rush to respond without checking if the message is real. For example, email titles like "Urgent! Limited-time offers inside" make people feel like the chance is rare, so they act fast. This works because people don't want to miss out or lose something, which makes them easier to trick (Lipscombe, 2024).



2. Authority

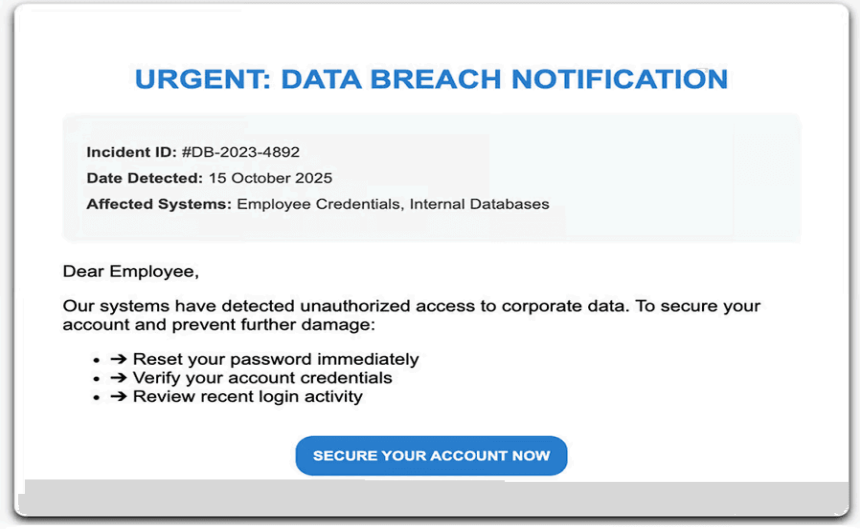
Attackers often pretend to be trusted groups like banks, government offices, or bosses at work to make people trust them. They use official-looking language and pretend to be familiar organizations to lower people's guard and get them to follow their requests. For example, phishing emails might look like real messages from a bank, using logos and branding to trick people into giving away their private banking

information. This use of trust takes advantage of how people tend to listen to authority figures, making it easier to fool them (Lipscombe, 2024).



3. Fear-Based Strategies

Attackers often use emotions to trick people into reacting quickly without thinking. They try to make people feel scared by sending messages that warn about serious problems, like losing access to their account unless they act fast and confirm their information. When people feel scared, they may stop thinking clearly and just follow the instructions without checking if the message is real. This method uses strong emotions to make people give away private information or click on dangerous links (Lipscombe, 2024).



III. NOTABLE PHISHING CAMPAIGNS

1. Google and Facebook Phishing Scam (2013-2015)

Between 2013 and 2015, a Lithuanian fraudster named Evaldas Rimasauskas orchestrated a phishing campaign that deceived both Google and Facebook into transferring over $100 million. Rimasauskas impersonated Quanta Computer, a legitimate Taiwanese supplier to both companies, sending fake invoices and contracts. Employees at Google and Facebook processed these payments, believing they were legitimate business transactions. The scam was eventually uncovered, leading to Rimasauskas' arrest and extradition to the United States. Both companies recovered approximately $49.7 million of the stolen funds (Huddleston, 2019).

2. Crelan Bank Business Email Compromise (2016)

In 2016, Belgium's Crelan Bank fell victim to a Business Email Compromise (BEC) attack, resulting in a loss of approximately €75.8 million. Attackers compromised the email account of a high-level executive and sent fraudulent instructions to employees, directing them to transfer funds to accounts controlled by the attackers. The scam was discovered during an internal audit, highlighting vulnerabilities in email communication and financial transaction processes (Pindrop, 2025).

COMPARATIVE ANALYSIS

CRITERIA	SQL INJECTION	PHISHING
Attack Vector	**Technical**: Exploits vulnerabilities in web applications that fail to properly sanitize user input.	**Human-centric**: Exploits human psychology (e.g., urgency, authority, trust).
Examples	- Heartland Payment Systems (2008) - Sony Pictures (2011)	- Google and Facebook Scam (2013–2015) - Crelan Bank BEC Attack (2016)

Method of Execution	Injection of malicious SQL code into input fields (e.g., login forms, search bars) to manipulate databases.	Social engineering via email, impersonation, or fake login pages.
Complexity of Execution	**Medium to High**: Requires knowledge of SQL, database structures, and web security flaws.	**Low to Medium**: Requires research and psychological manipulation, but not deep technical skills.
Primary Target	**Systems**: Web servers and applications with weak input validation.	**Humans**: Employees, executives, or end-users who can be socially engineered.
Impact on Organizations	- Massive data breaches (e.g., Heartland: 130M+ card numbers, Sony: 1M+ user records)	- Financial loss (e.g., Google/Facebook: $100M, Crelan Bank: €75.8M) - Reputation damage
Impact on Individuals	- Exposure of personal data (e.g., passwords, financial records), risk of identity theft.	- Victims may suffer identity theft, financial fraud, or job loss due to internal compromise.
Detection & Prevention Difficulty	Can be detected with code audits and input sanitization; preventable with secure coding practices.	Often hard to detect early; relies on user awareness and email filtering systems.
Recovery Complexity	High: Data recovery, system patching, and long-term damage control (especially if data is leaked).	Medium: Financial recovery may be possible; reputational damage is harder to repair.

SQL Injection attacks are more technical and require deeper knowledge of web development and database systems, but they can cause massive data breaches if successful while the Phishing attacks manipulate human behavior and are easier to execute on a large scale using emails or fake websites. Their success depends on the psychological pressure placed on victims. Both types of attacks are highly damaging, but they exploit very different weaknesses,people vs. code.

MITIGATION AND PREVENTION STRATEGIES

1. SQL Injection Prevention

STRATEGY	DESCRIPTION
Input Validation	Always check what users type into forms or search boxes. Make sure it only includes the kind of information you expect (like letters or numbers) and not special characters used in attacks.
Parameterized Queries	Don't let user input be part of a direct SQL command. Instead, use special tools (like prepared statements) that keep user input and commands separate. This stops attackers from running harmful code.
Object-Relational Mapping	These tools help developers work with databases safely by handling the behind-the-scenes code. Examples are Hibernate or Django ORM. They make it harder to write unsafe SQL commands.
Regular Code Reviews	Regularly check your code to find and fix any weak spots before attackers do.

2. Phishing Prevention

STRATEGY	DESCRIPTION
User Education	Train employees to spot suspicious emails, links, and requests for private info. Help them understand how phishing works.
Multi-Factor Authentication	Even if someone steals a password, they can't log in without the second step, like a code sent to your phone.
Usage of Email Filters	Set up systems that catch and block suspicious emails before they reach people's inboxes.

Intrusion Detection Systems	These systems watch for unusual activity in your network and help stop attacks early.
Audits	Frequently check your systems and emails for any weak points or signs of attacks.

ETHICAL CONSIDERATIONS

Researching cybersecurity problems like SQL injection and phishing comes with serious ethical responsibilities. These problems can lead to big issues like stolen personal data, lost money, or broken trust between users and companies. Finding these problems can help make systems safer, but what really matters is how the information is handled. If a researcher shares details about the weakness before telling the company, hackers might use it to cause harm (Finn, 2020).

To avoid this, many experts follow a process called Responsible Disclosure or Coordinated Vulnerability Disclosure. This means the researcher tells the company about the problem in private first, so they have time to fix it. For example, if someone finds an SQL injection issue on a company's website, they should report it to the company, not post it online. The same goes for phishing: if someone finds an easy way to trick users through email, they should quietly let the affected company know (Scarfone & Mell, 2007).

Researchers also need to follow the law. Testing a website or email system without permission even for good reasons can be illegal. For example, trying out SQL commands on a real website to find bugs, or sending fake phishing emails to users, might break rules. Ethical researchers should use official guidelines, like the ones from the Computer Emergency Response Team (CERT) or the International Organization for Standardization (ISO). In the end, researching SQL injection or phishing isn't just about finding the problem. It's about doing the right thing with the information. Good researchers protect people, help companies fix issues, and make the internet a safer place for everyone.

TRENDS

Data from recent years shows a clear increase in cyberattacks, especially phishing, which has become one of the most common threats online. One major spike in phishing happened during the COVID-19 pandemic, when many people were working from home and using digital tools more often. Attackers took advantage of this change in behavior.

The FBI's Internet Crime Complaint Center (IC3) reported that phishing was the most common cybercrime in 2021, with 323,972 complaints, compared to 114,702 in 2019—almost three times more in just two years (FBI, 2022). This shows how quickly phishing grew during the pandemic.

In 2020, a report by Proofpoint found that over 70% of organizations saw phishing emails that used COVID-19 topics to trick people. Many of these messages claimed to be from trusted sources like the World Health Organization (WHO) or local governments, asking people to click links or give personal details (Proofpoint, 2021). These fake messages used fear, urgency, or offers of help to make people act without thinking.

At the same time, SQL injection (SQLi) attacks showed a slight decline in frequency. One reason is that developers are using better security practices like input validation and prepared statements. However, SQLi still happens, especially on older websites that haven't been updated. According to Imperva's 2023 Threat Report, SQL injection still accounts for over 8% of all web application attacks, showing that it remains a risk, especially when software is not properly maintained (Imperva, 2023)

REFERENCE

Acunetix. (2023). *What is blind SQL injection?* https://www.acunetix.com/blog/articles/blind-sql-injection/

Bferrite, & Bferrite. (2015, May 14). *Analysis of the Havij SQL Injection tool*. Check Point Blog. https://blog.checkpoint.com/security/analysis-havij-sql-injection-tool/

Cyber Security Unity. (2025, February 18). *Types of Cyber Attacks | Comprehensive Guide by Cyber Security Unity*. https://csu.org.uk/types-of-cyber-attack/

FBI. (2022). *Internet Crime Report 2021*. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Finn, P. (2020). *Ethics in cybersecurity research and practice*. *Journal of Cybersecurity, 6*(1), 1–9. https://doi.org/10.1093/cybsec/tyaa005

Heartland breach: Inside look at the plaintiffs' case. (n.d.). https://www.bankinfosecurity.com/heartland-breach-inside-look-at-plaintiffs-case-a-1844?utm

Huddleston, T., Jr. (2019, March 27). *How this scammer used phishing emails to steal over $100 million from Google and Facebook*. CNBC. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Imperva. (2023). *Cyber Threat Index Report*. https://www.imperva.com/resources/resource-library/reports/

Jain, A. K., & Gupta, B. B. (2018). *Phishing detection: Analysis of visual similarity-based approaches*. Security and Privacy, 1(1), e9. https://doi.org/10.1002/spy2.9

Kosinski, M. (2025, April 15). Smishing. *What is smishing (SMS phishing)?* https://www.ibm.com/think/topics/smishing

Lipscombe, S. (2024, March 26). *The Psychology of Phishing: Recognizing and Avoiding Scams*. Wizard Cyber. https://wizardcyber.com/the-psychology-behind-phishing-attacks/

Najera-Gutierrez, G., & Ansari, J. A. (n.d.). *Web Penetration Testing with Kali Linux - Third Edition*. O'Reilly Online Learning. https://www.oreilly.com/library/view/web-penetration-testing/9781788623377/a8afd0e8-9782-40a2-a454-b04f5e0124f2.xhtml

OWASP. (2023). *SQL Injection.* https://owasp.org/www-community/attacks/SQL_Injection

OWASP. (2023). *OWASP top ten: Injection and phishing risks.* https://owasp.org/www-project-top-ten/

Proofpoint. (2021). *2021 State of the Phish Report*. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Pindrop. (2025, January 20). *CEO phishing scam costs Belgian bank Crelan $75M - Pindrop*. https://www.pindrop.com/article/ceo-phishing-scam-costs-belgian-bank-crelan/

Poulsen, K. (2011, June 2). Sony hit yet again; consumer passwords exposed. *WIRED*. https://www.wired.com/2011/06/sony-lulzsec/?utm

PortSwigger. (n.d.). *Blind SQL injection*. https://portswigger.net/web-security/sql-injection/blind

PortSwigger. (n.d.). *Union-based SQL injection*. https://portswigger.net/web-security/sql-injection/union-attacks

Robinson, S., Lutkevich, B., & Clark, C. (2024, November 18). *What is a whaling attack (whaling phishing)?* Search Security. https://www.techtarget.com/searchsecurity/definition/whaling

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Sharadin, G. (2023, December 21). What is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva. Learning Center. https://www.imperva.com/learn/application-security/sql-injection-sqli/

Secure Email Threat Defense demo. (2025, April 10). [Video]. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-vishing.html

sqlmap: automatic SQL injection and database takeover tool. (n.d.). https://sqlmap.org/

SQL injection & how to prevent it. (2025, March 19). https://www.kaspersky.com/resource-center/definitions/sql-injection

What is phishing? - meaning, attack types & more | ProofPoint US. (2025, April 18). Proofpoint. https://www.proofpoint.com/us/threat-reference/phishing

What is spear phishing? - Definition, Examples, prevention | ProofPoint US. (2025, March 5). Proofpoint. https://www.proofpoint.com/us/threat-reference/spear-phishing

What is SQL Injection? Tutorial & Examples | Web Security Academy. (n.d.). https://portswigger.net/web-security/sql-injection

APPENDICES

A. **Appendix A: Union-based SQL Injection Example**

   Copy Edit ' UNION SELECT username, password FROM users --

B. **Appendix B: Error-based SQL Injection Example**

   Copy Edit ' OR 1=1 ORDER BY 100 –

C. **Appendix C: Blind SQL Injection Example**

   Copy Edit ' AND 1=1 --

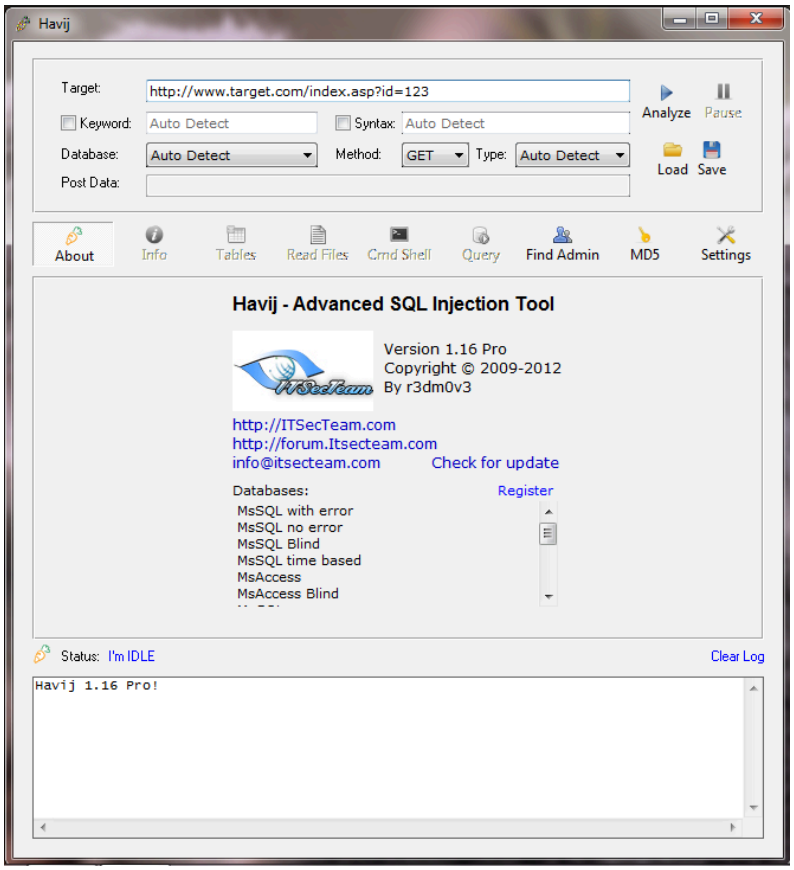
D. **Appendix D: Time-based SQL Injection Example**

   Copy Edit ' IF(1=1, SLEEP(5), 0) --

E. Appendix E: SQLMap Screenshot

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.4.44#dev}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

F. Appendix F: Havij Screenshot

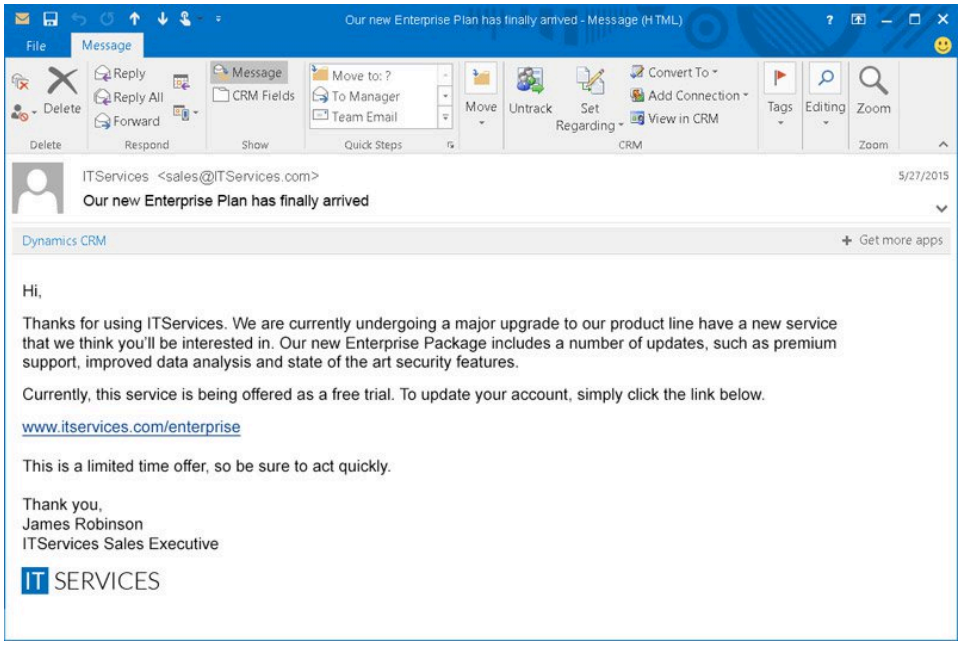


G. Appendix G: SQLNinja Screenshot

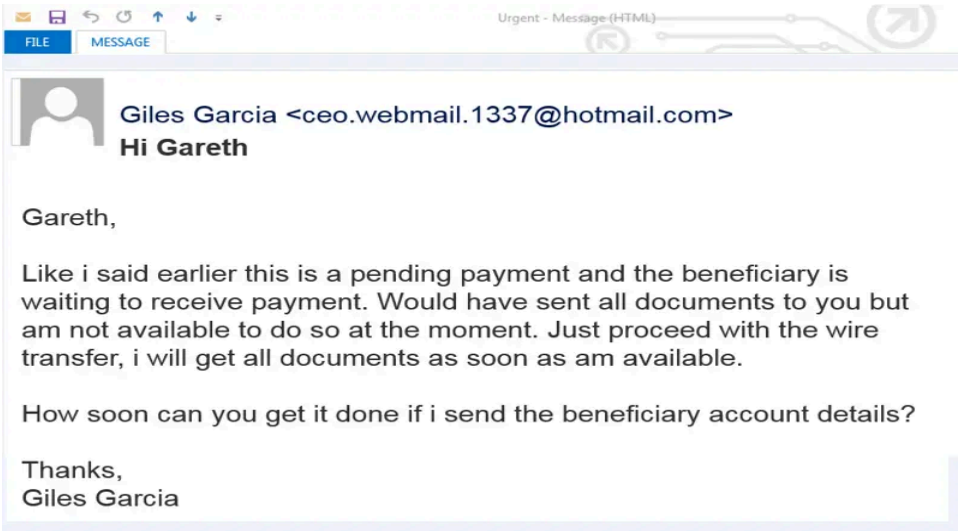
```
What do you want to discover?
  0 - Database version (2000/2005/2008/2012)
  1 - Database user
  2 - Database user rights
  3 - Whether xp_cmdshell is working
  4 - Whether mixed or Windows-only authentication is used
  5 - Whether SQL Server runs as System (xp_cmdshell must be available)
  6 - Current database name

  a - All of the above
  h - Print this menu
  q - quit
 > 2
[+] Checking whether user is member of sysadmin server role....
    You are an administrator!
 > 3
[+] Checking whether xp_cmdshell is working....
    xp_cmdshell is working!
 > 5
[+] Checking whether SQL Server runs as NT Authority\SYSTEM...
    SQL Server does not appear to be running as System. You can try
    uploading and using churrasco.exe to attempt token kidnapping
 >
```

enumerating users and privileges

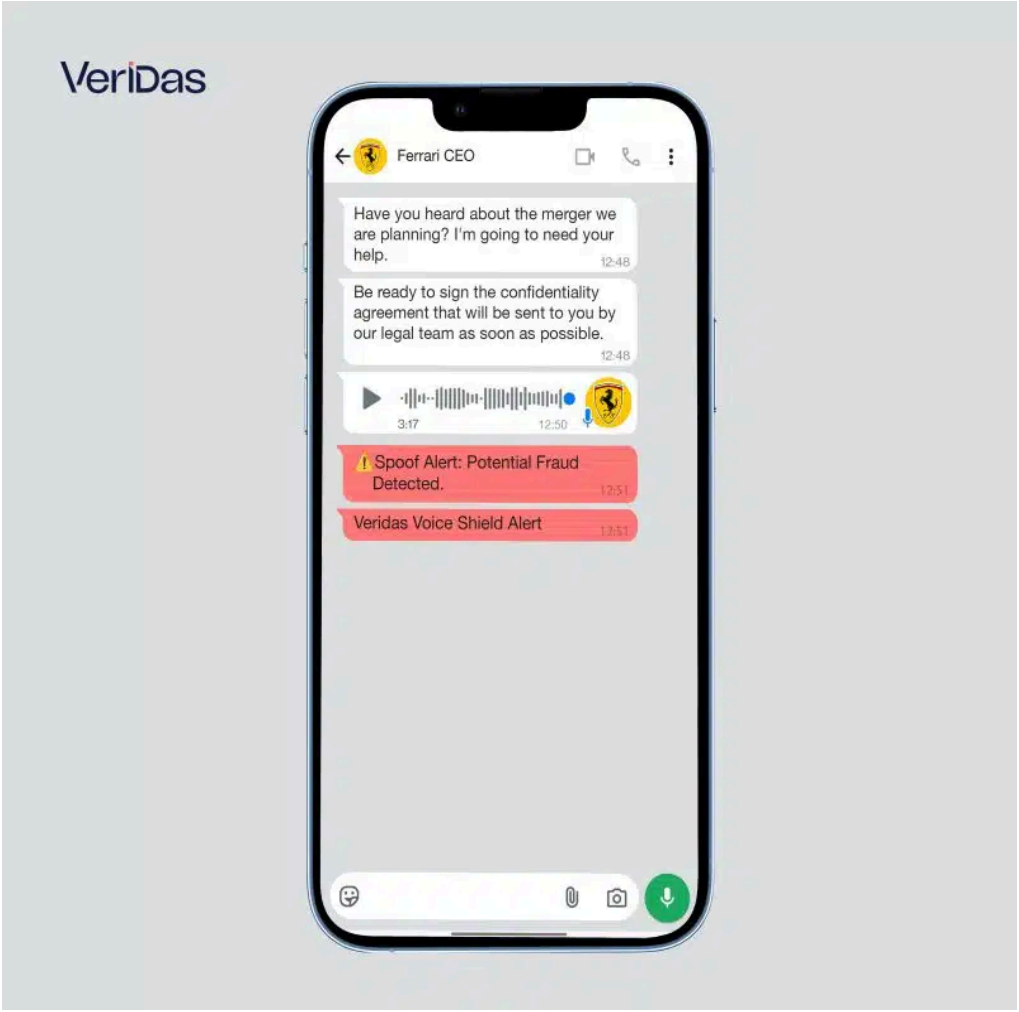
H. Appendix H: Spear Phishing Example



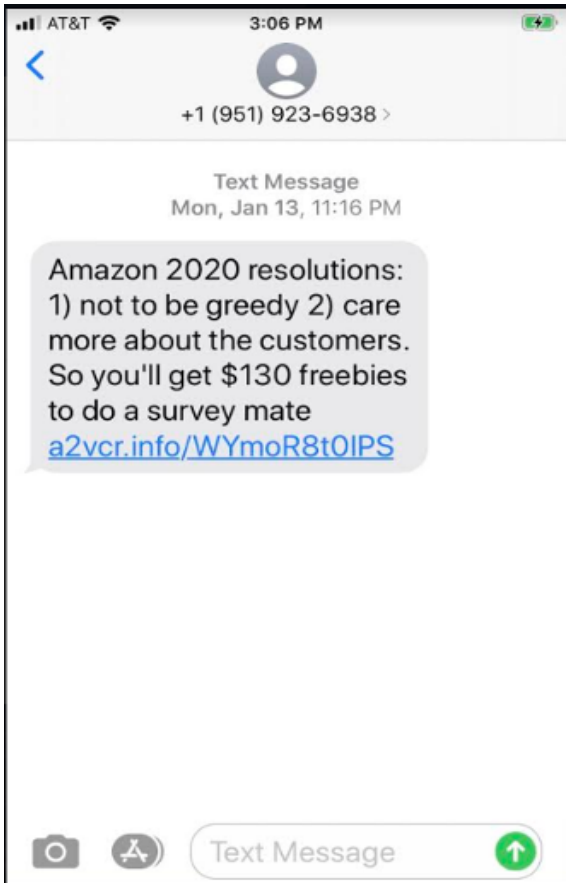
I. Appendix I: Whaling Example



J. Appendix J: Vishing Example



K. Appendix K: Smishing Example



L. Appendix L: Urgency Psychological Tactic Example

From: *(A familiar name, often a supervisor)*@gmail.com>
Sent: Wednesday, February 27, 2019 12:36 PM
To: *(Email may be sent to a list of people, including people you know)*

Subject: URGENT REQUEST

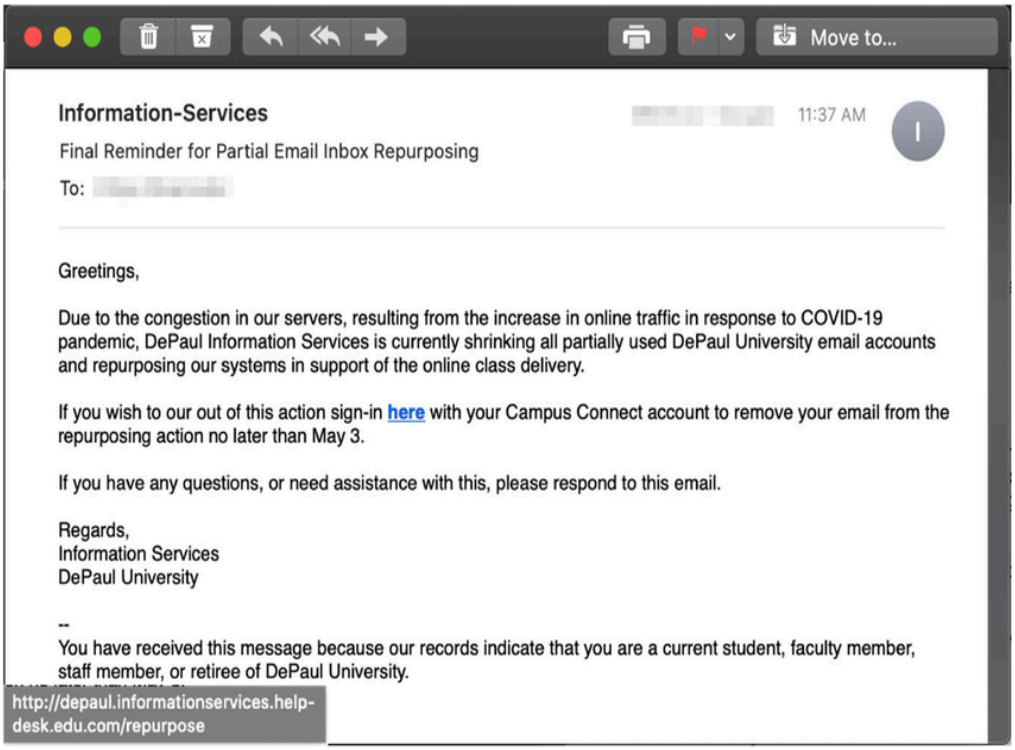
Hi,Got a moment?Give me your personal cell number.I need you to complete a task for me

Thanks

(A familiar name, often a supervisor often a person in a leadership position)
Professor of Accounting

Sent from my iPhone

M. Appendix M: Authority Psychological Tactic Example



N. Appendix N: Fear Psychological Tactic Example