Phishing Simulation

Proposal for phishing simulation: intel.com

Feb' 2024

Prepared by :

Gopi Gor

FDIN: A21370441

ggg@fordham.edu

Executive Summary

Headquarted in Santa Clara, California, Intel is known to be a global technology company, mainly in semiconductors and computing technology. It made the first microprocessor in 1971 and has been raising the bar with new influential products.

The importance of cybersecurity today, is as important as the act of locking one's door in olden times. The most emerging trends in 2024 in cybersecurity are Phishing Scams, AI Potential, Cloud, Social Engineering, Insider Threats, MFA, Automotive Hacking, and Ransomware. All of these could cause huge losses to a business.

Phishing is emerging as the most powerful tool today for adversaries to hack into a network, organization or obtain PII. Phishing is usually done by sending legitimate looking emails to people who fall trap and click on links that execute malicious code to obtain information.

This report conducts 3 different methods of phishing simulations for the company intel.com to understand if employees fall prey to these phishing simulations.

1. General Email Phishing

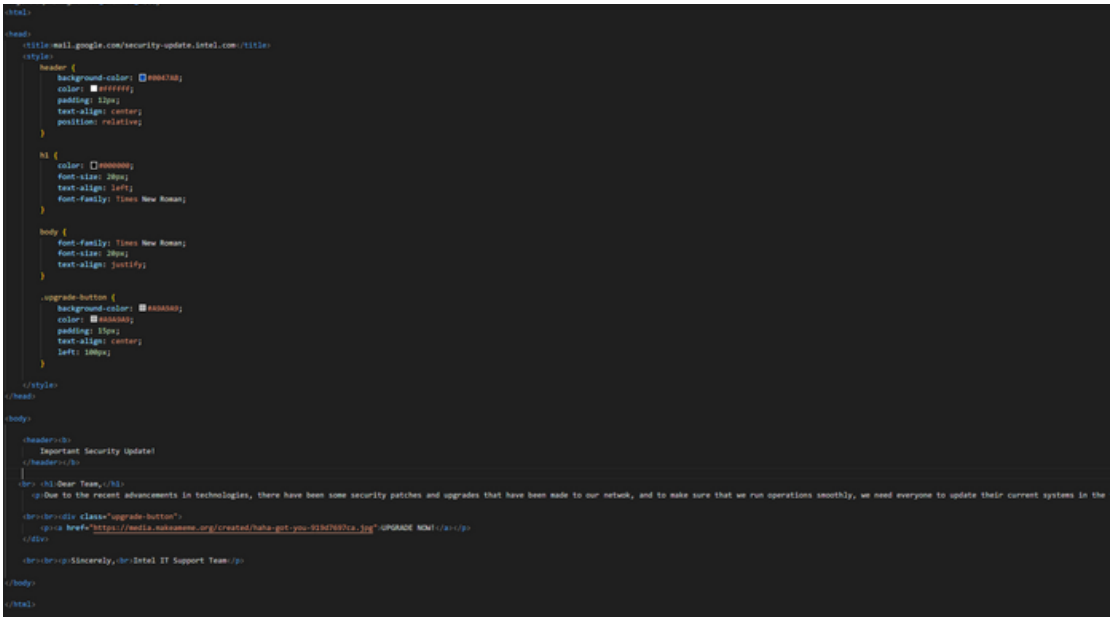
The general phishing technique we used in this simulation is a basic security upgrade sent from the IT team at Intel. The template is like a very simple banner and a message that is addressed to the team. There is a link at the bottom which says “Upgrade Now!”. The thought process behind this was to create a very legitimate-looking and convincing email that users believe has come from the IT team.

When a user clicks on the upgrade now button, it takes them to another link/page which can have malicious files on it, or .exe files which get executed the minute the link is clicked.

To understand how and why this email is malicious, it is evident, that the email says to upgrade in the next “3 hours”. This creates a sense of urgency, in order to not put the organization in any danger. Furthermore, the link to upgrade creates further sense of urgency with the “UPGRADE NOW!” text. If carefully looked, there is a part in the email which repeats the word “the” two times. Organizations that are handling complex networks, will make sure that there are no errors whatsoever in any email sent. There is no contact information given which makes it more suspicious.

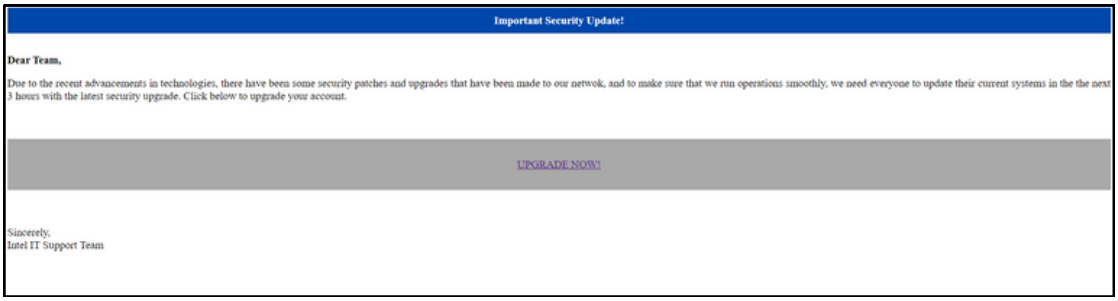
(HTML code and screenshots attached below)

1.General Email Phishing



```
<html>

<head>
    <title>mail.google.com/security-update.intel.com</title>
    <style>
        header {
            background-color: #0047AB;
            color: #ffffff;
            padding: 12px;
            text-align: center;
            position: relative;
        }

        h1 {
            color: #000000;
            font-size: 20px;
            text-align: left;
            font-family: Times New Roman;
        }

        body {
            font-family: Times New Roman;
            font-size: 20px;
            text-align: justify;
        }

        .upgrade-button {
            background-color: #A9A9A9;
            color: #A9A9A9;
            padding: 15px;
            text-align: center;
            left: 100px;
        }

    </style>
</head>

<body>

    <header><b>
        Important Security Update!
    </header></b>

    <br> <h1>Dear Team,</h1>
        <p>Due to the recent advancements in technologies, there have been some security patches and upgrades that have been made to our netwok, and to make sure that we run operations smoothly, we need everyone to update their current systems in the

    <br><br><div class="upgrade-button">
        <p><a href="https://media.makeameme.org/created/haha-got-you-910d7697ca.jpg">UPGRADE NOW!</a></p>
    </div>

    <br><br><p>Sincerely,<br>Intel IT Support Team</p>

</body>

</html>
```

Fig.1: HTML Code



Important Security Update!

Dear Team,

Due to the recent advancements in technologies, there have been some security patches and upgrades that have been made to our netwok, and to make sure that we run operations smoothly, we need everyone to update their current systems in the the next 3 hours with the latest security upgrade. Click below to upgrade your account.

UPGRADE NOW!

Sincerely,
Intel IT Support Team

Fig.2: Phishing Email Preview

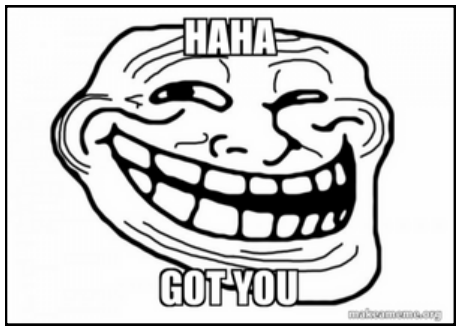


Fig.3: Landing page for “UPGRADE NOW”

2.Spear Phishing

The spear phishing technique and the thought process behind this simulation was focused on one specific individual in the company. In this case, the CTO of the company reached out to an employee, telling them with a surprise that they have been promoted via the subject line. This is a compelling reason to open the email, and works on the pyschological aspect of human mind. It tells the employee to fill out details to confirm the offer and fill out the required paperwork.

When the employee clicks on the link in the email, it takes them to form like page, where he then enters his details. When he clicks submit, it takes him to another page, which could mean his details have been captured. From hereon, his details can be used anywhere.

To understand how and why this email is malicious, firstly, the employee in this scenario could have been employed for only few months and furthermore, employee is never directly sent an email. It is informally said in conversations. Secondly, if we look at the email body, there is an error for the effective date as the promoted new position. This shows an error by the adversary because the date received of the email is the same day Feb 3rd, but the effective date is December 2023.

(HTML code and screenshots attached below)

2.Spear Phishing

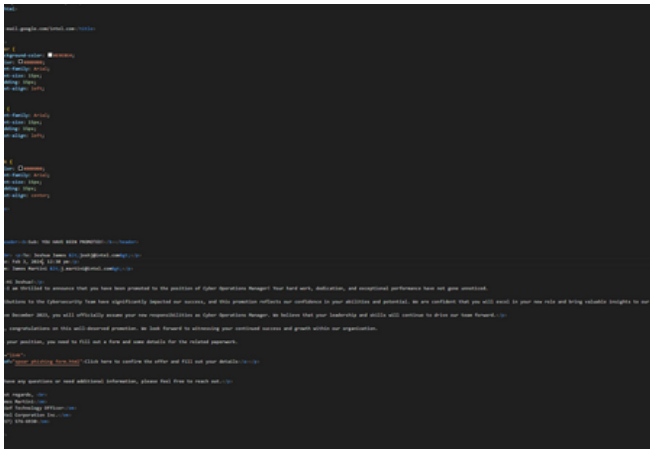
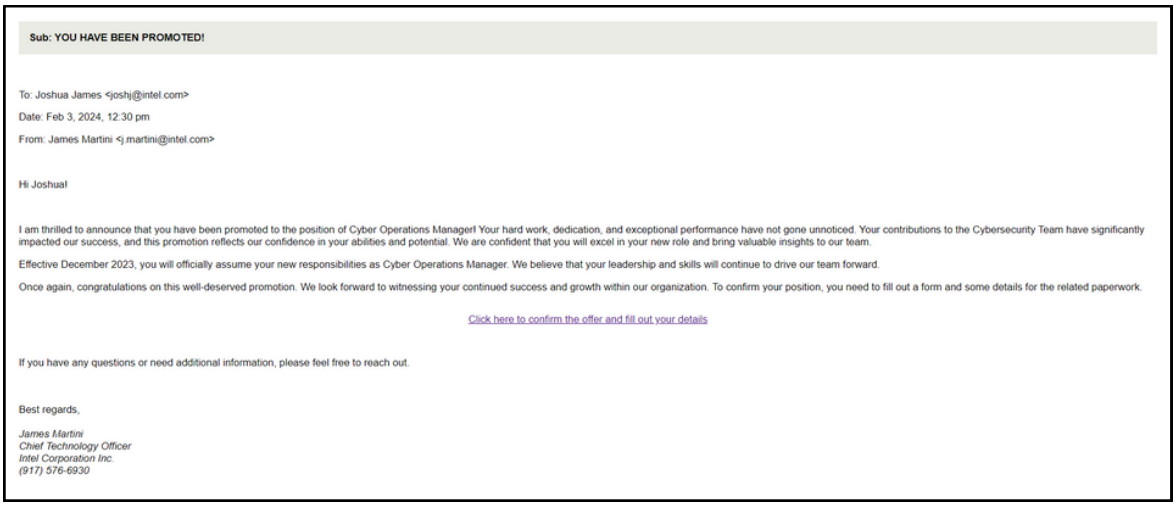


Fig.1: Email HTML Code

Fig.2: Form HTML Code



Sub: YOU HAVE BEEN PROMOTED!

To: Joshua James <joshj@intel.com>

Date: Feb 3, 2024, 12:30 pm

From: James Martini <j.martini@intel.com>

Hi Joshua!

I am thrilled to announce that you have been promoted to the position of Cyber Operations Manager! Your hard work, dedication, and exceptional performance have not gone unnoticed. Your contributions to the Cybersecurity Team have significantly impacted our success, and this promotion reflects our confidence in your abilities and potential. We are confident that you will excel in your new role and bring valuable insights to our team.

Effective December 2023, you will officially assume your new responsibilities as Cyber Operations Manager. We believe that your leadership and skills will continue to drive our team forward.

Once again, congratulations on this well-deserved promotion. We look forward to witnessing your continued success and growth within our organization. To confirm your position, you need to fill out a form and some details for the related paperwork.

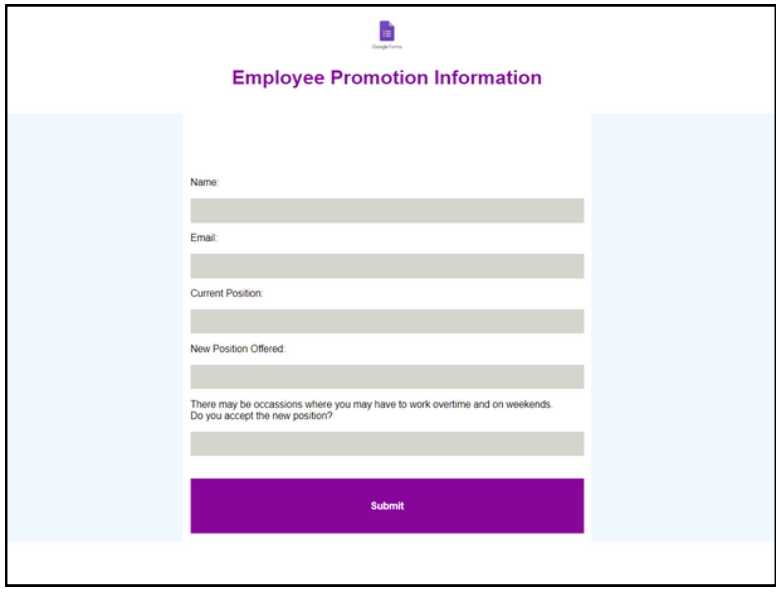
Click here to confirm the offer and fill out your details

If you have any questions or need additional information, please feel free to reach out.

Best regards,

James Martini
Chief Technology Officer
Intel Corporation Inc.
(917) 576-6930

Fig.3: Phishing Email Preview



Employee Promotion Information

Name:

Email:

Current Position:

New Position Offered:

There may be occassions where you may have to work overtime and on weekends.
Do you accept the new position?

Submit

Fig.4: Landing page for “click here for form”

Fig.5: Landing page for Submit

3.Whaling Phishing

The whaling phishing technique in this simulation is aimed at the CFO of the company and plays with the authoritative part of the position. The finance manager reaches out to the CFO to approve a big payment, by logging into the bank through a link and provides details for the same. This plays on the CFO mind with the urgent request. The mail is structured in a way that shows that the CFO knows about the transaction. It's considered a whaling because a CFO is like the big whale, with all the money, and a phishing attempt against him could earn the attacker lots of money.

When the CFO clicks on the link in the email, it takes him to the Bank of America login page (I almost tried to make it similar) where he then enters his User ID and Password. When he clicks submit, it takes him to another page, which could mean the fake Bank of America page could have a keylogger executed. From hereon, his details can be captured on every website he visits.

To understand how and why this email is malicious, firstly, the email id is not right with the initials of the sender wrong, and its not intel.com but intel.om. The subject line says URGENT Payment Request. The CFO may click on it due to subject line and out of office situations. The next page, has the login button not clear. The 'Forgot your password' also links randomly.

(HTML code and screenshots attached below)

3.Whaling Phishing

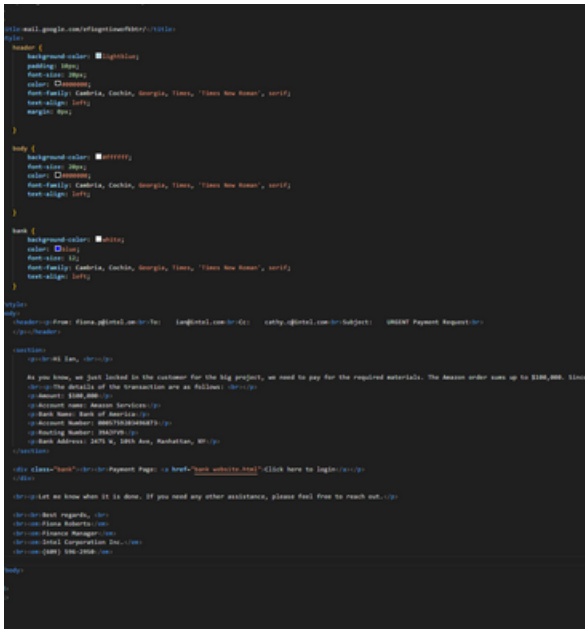


Fig.1: Email HTML Code

Fig.2: BoA HTML Code

Fig.3: Email Preview

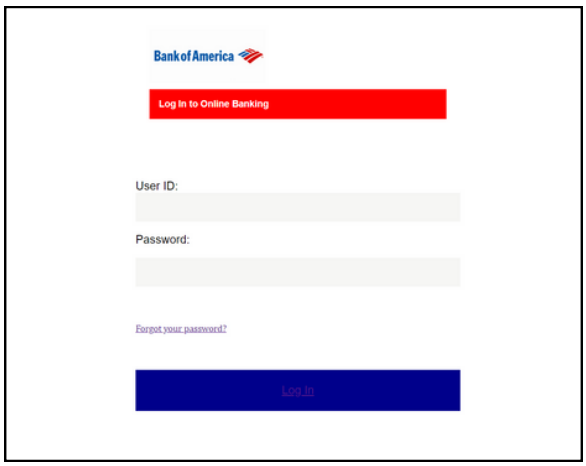


Fig.4: Landing Page BoA Preview

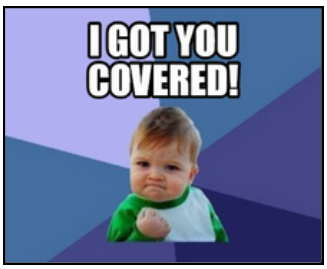


Fig.5 & 6: Landing Pages for Log In and Forgot Your Password