CW technology

LEARN HOW IT WORKS

RECOGNIZING & PREVENTING PHISHING SCAMS

Katherina Yavela
Marketing Coordinator

CW technology

TABLE OF CONTENTS

AUTHOR'S NOTE 2

INTRODUCTION 3

CHAPTER 1 4

CHAPTER 2 5

CHAPTER 3 6

CONCLUSION 7

AUTHOR'S NOTE

Katherina Yavela is the Marketing Coordinator at CW Technology.

A recent 2020 college graduate and new member to the CW team (as of June 2020), she brings passion, creativity, and resilience in growing our brand name, image, and awareness.

With an extensive marketing background and well-rounded set of experiences, Katherina has introduced a newfound perspective on marketing the IT and MSP industry. Her lack of a technical background doesn't stop her from learning and understanding the world of technology and the tremendous importance it holds, especially today.

At CW Technology, Katherina's role is building the brand across numerous marketing platforms, making the industry both relevant and reachable to all.

When not at work, Katherina enjoys reading, cooking, and learning Italian, which happens to be her fourth language!

INTRODUCTION

Since moving to remote work, all of us have become more susceptible and vulnerable to cyber attacks and cyber criminals. Be it for work or simply purchasing groceries, we now share more and more of our most valuable, personal information online (i.e. name, address, social security number, driver's license, credit card, etc.). Out of all cyber attacks, the most common and the one everyone must be extra prepared for is phishing.

If you fall for a phishing scam, not only are you personally hurt (i.e. stolen identity, money, etc.), but it hurts your company just as much, if not more (i.e. damaged reputation, diminished brand equity, client loss, costly expenses, etc.).

WHY IT MATTERS

Being locked away at home does not make any of us safe from cyber security attacks, especially when it comes to phishing scams.

Cyber criminals are taking full advantage of the COVID-19 pandemic as a platform to convince people to share their personally identifiable information, account credentials, and most valuable data. Since the hit of COVID-19 in the U.S., there have been:

- **240 million COVID-19 related spam phishing emails (sent daily).**
- **46% increase in phishing attacks.**
- **$12 million lost by organizations and individuals due to COVID-19 related phishing.**

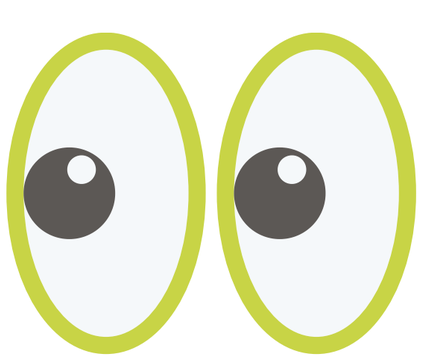
CHAPTER 1

RECOGNIZING PHISHING SCAMS

Phishing is an online scam, usually in the form of an email (also in the form of text messages and advertisements), where cyber criminals present themselves as a legitimate operation/organization to access and steal your valuable data.

Common COVID-19 related phishing emails ask users to click on an embedded link or download an attachment, and input personal information. The moment a user interacts with such an email, they give the cybercriminal complete control and access to the user's valuable data and credentials.

A PHISHING EMAIL IS...

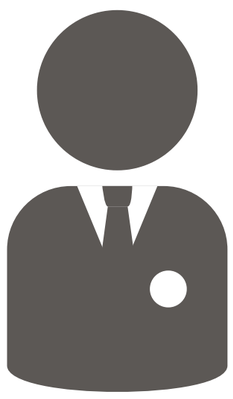


SUSPICIOUS

- Is sent from an unknown and unverified sender's email address - one you do not recognize.
- Is grammatically incorrect and has multiple spelling errors.
- Includes random and unverified links and/or attachments.

MANIPULATIVE

- Uses threatening language and/or instills panic.
- Requests and/or forces to click on a link or download an attachment.
- Is strategically written for reader to immediately carry out an action.



PERSONABLE

- Asks to confirm personal information.
- Asks to confirm financial information.
- Asks to change password or input credentials.

CHAPTER 2

CATCHING A PHISHING SCAM

If you have come across a phishing email in your inbox, it is important you know how to protect yourself. Simply put: **do not interact with it in any way.** Instead, follow these steps:

DO:

- **Delete and report immediately.**
- **Protect your device with anti-virus and anti-malware software.**
- **Check the email address.**
- **Determine if information request is actually appropriate/relatable.**
- **Check for incorrect grammar and spelling errors.**
- **Visit website by typing domain in yourself.**
- **Check the link before clicking on it.**

DO NOT:

- **Open and/or reply to the email.**
- **Click on any links.**
- **Open or download any attatchments.**

CHAPTER 3

WHAT IF I AM ALREADY A VICTIM?

So, the worst case scenario has happened: you interacted with a phishing scam! First things first - **do not to panic.** Depending on the type of scam, there are several, steps to take to safely recover and move forward. Let's take a look at a few, common phishing scams and what you should do if you accidently interact with one:

FAKE LINK OR LOGIN SCAM:

1. Change your password immediately.

2. Check for any mail rules that may have been set.

3. Check to make sure no email forwards are setup.

4. Run a malware cleaner (i.e. *Super Antispyware*, *Malwarebytes*).

5. If your company uses *Office 365*, have them log you out of all devices.

6. Black list the sender's address in your mail filter to prevent them sending messages to your organization.

FAKE EMAIL:

1. Change all applicable information.

2. Inform everyone in the organization about fake emails circulating.

3. Black list the sender's address in your mail filter to prevent them sending messages to your organization.

4. If any money or gift cards were given, contact your local police department.

CONCLUSION

As we continue to face the unknown about whether we will ever return to the work-office environment, there is one thing we can be certain about: phishing attacks are not going anywhere.

At ***CW Technology***, we provide the necessary and extensive information, protection, and training that you and your business needs.

If you have already experienced, or are worried about, increased phishing attacks, then contact us today to discuss how we can implement the optimal security processes and tools for you!

Duluth, Minnesota

5614 Grand Avenue, Duluth MN 55807
(218) 728 - 6000

Plymouth, Minnesota

2415 Annapolis Lane N, Suite 100, Plymouth MN 55441
(952) 544- 5400

Grand Rapids, Minnesota

212 N Pokegama Ave., Grand Rapids MN 55744
(218) 728 - 6000