GCyber-Corp

Beware of the Bait: Phishing Email Prevention

Author: Paul Gleason

Table of Contents

Table of Contents........1
Disclaimer........1
Introduction........1
What is Phishing?........1
Identifying Phishing Emails........2
Suspicious Sender:........2
Urgent Requests:........2
Unfamiliar Links:........3
Attachments:........3
Spelling and Grammar:........3
Protect the Spread........3
What to Do if You've Been Phished........4
Reporting:........4
Reponse:........4
Extra Resources:........4

Disclaimer

This document is for internal use only at GCyber-Corp all rights to this document are owned by GCyber-Corp and is not for redistribution. The reader is responsible for their own actions and decisions based on the information contained in this document. By using or accessing this information on this document, the reader agrees to accept full responsibility for any and all risks, losses, damages, or harm that may arise from the following information and how they use it.

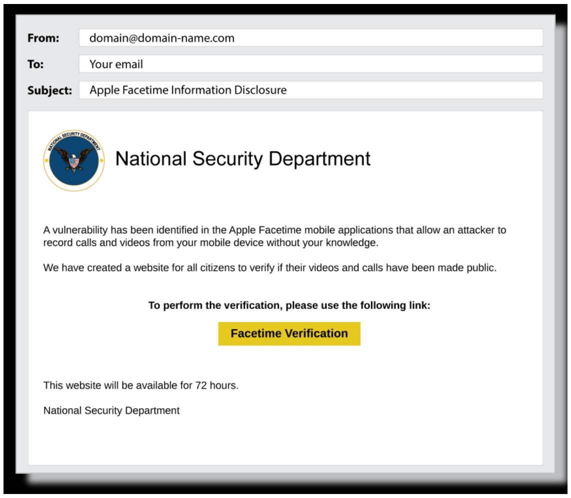
Introduction

At GCyber-Corp we have had an increase in phishing emails and would like to provide more information on how to avoid and protect yourself and the company. We have seen a hacker group called DragonFly spear heading many of their attacks towards our company. This document will outline what is phishing, how to identify a phishing email, and what to do if you have been phished or think you have a phishing email in your inbox.

GCyber-Corp

What is Phishing?

“Phishing is when attackers send malicious emails designed to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials or other sensitive data.” Proofpoint. Phishing emails can come in all shapes and sizes; some will look exactly like an email from a coworker or executive. Below are examples of a phishing email from Fortra’s Terranova Security. These emails show how easily phishing emails can blend in with every day work emails.



From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

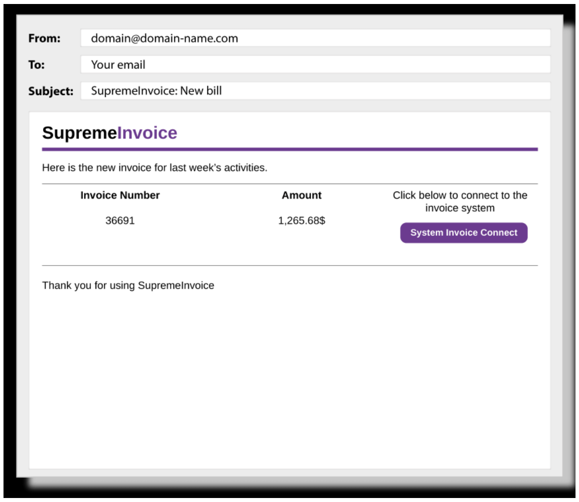
A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

This website will be available for 72 hours.

National Security Department



From: domain@domain-name.com

To: Your email

Subject: SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week’s activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	System Invoice Connect

Thank you for using SupremeInvoice

Identifying Phishing Emails

Below we will explain some of the ways phishing emails can be identified. There are many steps to take when identifying phishing emails. If you follow these steps below as though it’s a checklist it will increase your chances to spot and stop phishing emails.

Suspicious Sender:

If the sender is coming from an external source, always double check the email address. Phishing emails often have email addresses that closely resemble the companies email address or an address of a client or vender. For example our email is @gcyber-corp.org and a phishing email may use @gcyber-c0rp.org where they have replaced the “o” with a 0.

Urgent Requests:

Urgent emails demanding immediate action, like saying your account is compromised, you need to update information, you need to perform a security update. If you ever get an email saying your account is compromised it will be sent from cyber@gcyber-corp.org. Then all security updates will happen quietly in the background. We will never ask you to download or update anything through email. As well we will never ask for credential information through email.

Unfamiliar Links:

If you have been sent an email with hyperlinks this is where some text is blue and has a link attached to it. Before clicking on the link you can hover over the text it will show the true destination of the link. If hovering over the link doesn't show the location of where it will send you. You can right click on the text then select "copy linked address" doing this will let you then copy the link into a notepad to see where it will send you. Many attackers will make fake websites that will download unwanted/harmful software onto your computer when directed there, so it's always a good idea to triple check links.

Attachments:

When receiving an email with attachments make sure that you know the sender of the email as many attackers will place malicious attachments in emails. This may come in the form of an invoice, vendor requests, etc.

DragonFly has been seen sending emails with attachments as outlined by the CISA their attack preference is "Throughout the spear-phishing campaign, the threat actors used email attachments to leverage legitimate Microsoft Office functions for retrieving a document from a remote server using the Server Message Block (SMB) protocol. (An example of this request is: file[:]//<remote IP address>/Normal.dotm). As a part of the standard processes executed by Microsoft Word, this request authenticates the client with the server, sending the user's credential hash to the remote server before retrieving the requested file. (Note: transfer of credentials can occur even if the file is not retrieved.) After obtaining a credential hash, the threat actors can use password-cracking techniques to obtain the plaintext password. With valid credentials, the threat actors are able to masquerade as authorized users in environments that use single-factor authentication." CISA

Spelling and Grammar:

If an email has obvious poor grammar or spelling and the email is from an external sender this is a strong indication that the email is a phishing email.

Protect the Spread

To protect yourself and others we will outline a few steps below on what to do to make sure your account and computer are the safest they can be.

1. Multi-Factor Authentication: Enable multi-factor authentication (MFA) on your online accounts, which requires additional verification beyond a password, such as a text message code or fingerprint.
2. Use Strong, Unique Passwords: Create complex passwords for each of your online accounts and never reuse them. Consider using a password manager to help keep track of your passwords securely. You can use a password manager to keep track of those passwords, If you would like to use the password manager we provide please inquire at cyber@gcyber-corp.org.
3. Updates: keep your computer and applications up to date. When you're prompted for a restart for updates please do this at the end of your shift. This will ensure that security patches are pushed out as quickly as possible.

What to Do if You've Been Phished

Reporting:

If you haven't clicked on anything yet but believe you have a phishing email in your inbox please send it to cyber@gcyber-corp.org. Even if you're suspicious of an email we will always take a look at it. We would rather be safe than sorry. If you believe you have fallen for a phishing email please follow the steps below under "Reponse".

Reponse:

If you believe you have been compromised by a phishing email please report it to cyber@gcyber-corp.org with the subject of the email being "Account Compromised Phishing Email". This will give us an automatic notification with a process to follow. Below are the steps you will need to do after sending that email to cyber@gcyber-corp.org.

1. Reset Password for account https://passwordreset.gcyber-corp.org
2. Clear browser cache. Safari, Chrome, Firefox, Edge
3. Monitor for unwanted processes on the machine.

Extra Resources:

Federal Trade Commission Consumer Advice page on "How to Recognize and Avoid Phishing Scams"

Google's page on how to "Avoid and report phishing emails"

Security Metrics "7 Ways to Recognize a Phishing Email: Email Phishing Examples"

Zdnet "What is phishing? Everything you need to know to protect yourself from scammers"

NHS page on “DragonFly 2.0”

CISA Page on “DragonFly”