



THE UNIVERSITY OF  
**CHICAGO**

Biological Sciences Division  
**Information Security Office**

March 2024



## Cybersecurity Awareness Newsletter

Protecting yourself and information from cybersecurity threats.



It is Tax Season! Although the IRS will be accepting Federal tax returns until April 15<sup>th</sup> of this year, this looming deadline adds stress to our already busy lives. Money is a prime motivator for scammers to target unsuspecting individuals and they enjoy pretending to be the IRS or a collections agency so, this month I want to go over more phishing tips to help everyone stay safe while filing your taxes.





### Social Engineering Awareness

During tax season, many scammers use social engineering tactics to deceive and manipulate folks into giving up their sensitive confidential information by impersonating authorities. Their

goal is to create panic (via fear, curiosity or greed) and pressure you into revealing information, especially payment information.

Common scams and fraudulent phone calls often impersonate the IRS, however:

1) Very rarely will the IRS ever contact you by phone (unless you are being audited or owe lots of back taxes). The IRS will first attempt communication with you via post office mail. 

2) The IRS will never threaten you over the phone with legal action or to pay taxes immediately. These are intimidation tactics that scammer use often. 

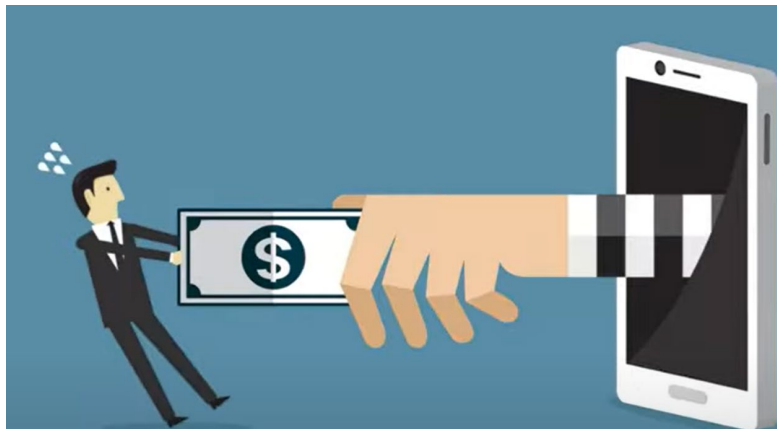
3) The IRS will never request gift cards as a method of payment.



4) The IRS will never ask for your credit card information over the phone.



Legitimate IRS interactions do not involve sharing sensitive information over the phone.

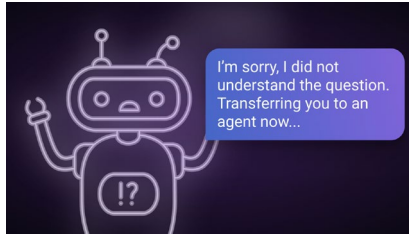


### Technology Awareness

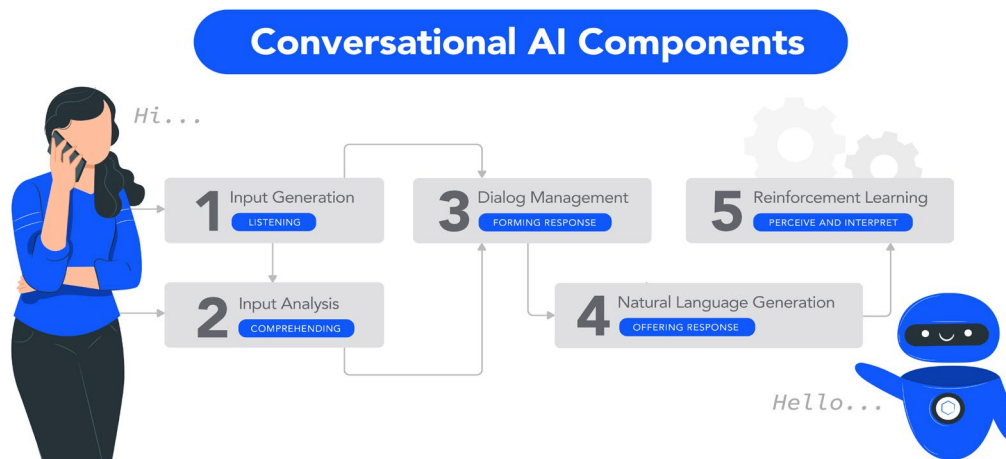
To help defend ourselves against new scam threats, we must understand the technology behind them. By understanding the mechanics of the fraudulent schemes, we gain insights into their tactics. Armed with this knowledge, we can recognize red flags, protect our information, and make informed decisions. Let's jump right in:

- Chat bots – Are not new. These have been around for years and have been used to simulate automated phone support responses, balance and bill notifications, on website chat bubble communications, order tracking from mail carriers, appointment scheduling, internal help desk systems and some help applications to input voice or text and output expected responses. These chat bots gave the illusion of understanding user input based

on predefined patterns, but given a pattern that it didn't understand it would sometimes just default to a predefined response.



- AI chat bots – Often referred to as Virtual Agents, are an evolution of old chat bots. They combine 3 different technologies (Statistical models, machine learning and computational linguistics) to provide a more seamless speech or text presentation by leveraging Artificial Intelligence techniques such as natural language processing (NLP) to provide responses. Some AI chat bots can even consider elevated voices, adapting to various tones, pitch, and emphasis to which they can provide empathetic responses. These chat bots can be used in both text based (email, phone text, chat apps) as well as voice based applications such as over a phone.



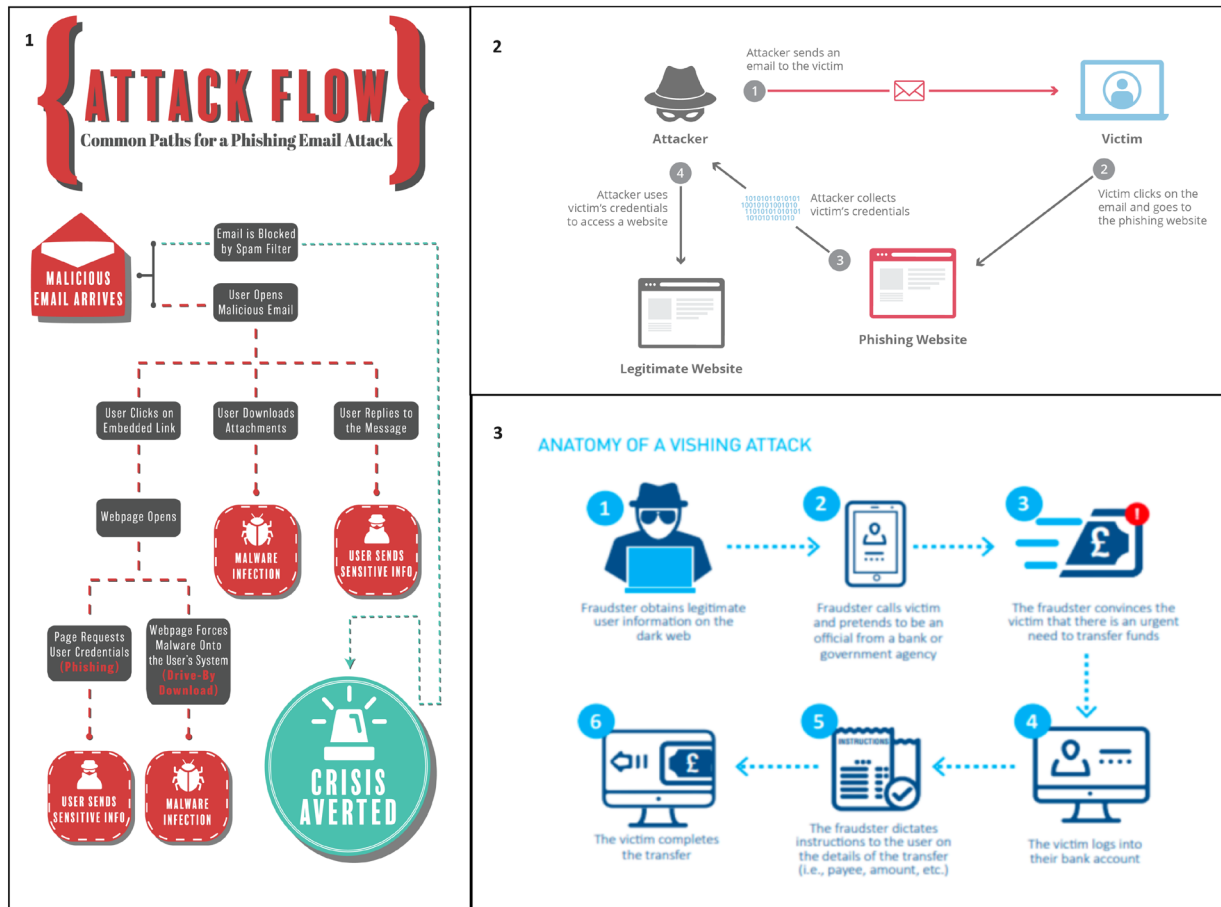
- In a previous newsletter we discussed AI video and voice generation. These methods also apply here: [https://bpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/3/3185/files/2023/11/Newsletter\\_November\\_2023\\_Final2.pdf](https://bpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/3/3185/files/2023/11/Newsletter_November_2023_Final2.pdf)

### Attack Flow Awareness

In a typical phishing and vishing attack the following steps usually occur:

- 1) **Initial Contact:** The attacker sends a phishing email or phone call to the victim.
- 2) **Deceptive Content:** The email or phone call relays deceptive content (urgent requests, fake login pages).
- 3) **Victim Interaction:** The victim interacts with the email or talks during the phone call (clicks a link, downloads attachment, engages in conversation with AI).
- 4) **Payload Delivery:** If successful, the attacker delivers a payload (malware, ransomware, etc.) if their objective is to take over your computing device or begins using your information to craft an identity theft response.
- 5) **Exploitation:** The payload exploits vulnerabilities on the victim's system or they decide to auction/sell your information on the dark web.
- 6) **Data Theft or Control:** The attacker gains unauthorized access, steals data, and/or gains control of assets.

### 3 Dataflow Examples



### The Ghost Tax Preparer

Other items that need emphasis: We mentioned “ghost” tax preparers last year and it is still relevant this year. If you are hiring a tax professional, work only with a legitimate and reputable Tax Preparer. You can validate a preparer’s credentials with the IRS here:

<https://irs.treasury.gov/rpo/rpo.jsf>



By law, anyone who is paid to prepare or assist in preparing federal tax returns must have a valid Preparer Tax Identification Number, or PTIN. Any preparer will have a PTIN you can use to

verify and check their reputation. Do not hire anyone who promises a high return and charges a fee based on the return. Avoid a “ghost preparer,” or someone who wants to make a fast buck and does not sign a tax return they prepare.

### **Reputable Websites**

Be aware of reputable websites that claim to be an organization they are not. To mitigate this risk here are a few tools to help you identify a malicious website before attempting to enter the website URL into your web browser:

<https://urlscan.io/>

<https://www.virustotal.com/gui/home/upload>

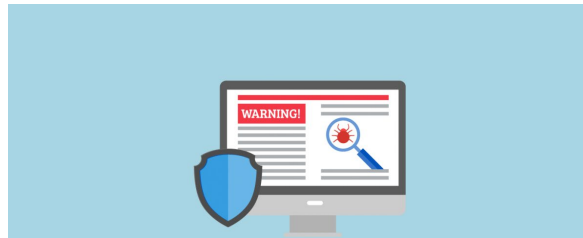
<https://www.hybrid-analysis.com/>

<https://radar.cloudflare.com/scan>

<https://webscan.upguard.com/>

<https://www.sitelock.com/free-website-scan/>

<https://www.ipqualityscore.com/threat-feeds/malicious-url-scanner>



These URL checkers analyze not only the potential risks but also help in making a holistic assessment of an organization associated with the site.

As always, we welcome your feedback and any suggestions for topics that you would like us to cover in the next newsletter. Please send us an e-mail at [security@bsd.uchicago.edu](mailto:security@bsd.uchicago.edu) .