THE UNIVERSITY OF CHICAGO | Biological Sciences Division Information Security Office

November 2023

Cybersecurity Awareness Newsletter

Protecting yourself and information from cybersecurity threats.

As the holidays approach, so do the retail ads for the biggest shopping event of the year. Black Friday deals have been popping up all year long, and they will only get more frequent and enticing as we get closer to the end of November and well into January. Cybercriminals don't waste this opportunity either, both online and offline during the shopping season. This year they have artificial intelligence (AI) tools at their disposal to create convincing content to trick us into revealing our sensitive information. In this month's newsletter, I'll discuss some of the clever scams that are being done and how to avoid them.

Compliance and Ethics

Before we start discussing AI schemes and scams, I wanted to draw your attention that earlier this month it was Corporate Compliance and Ethics week. We wanted to remind employees that are working with paper or electronic records, with or without sensitive information, should ensure that they comply with data record maintenance and retention policy found here:

A08-03 Record Maintenance and Retention.pdf (uchicagomedicine.org)

For questions or guidance regarding record maintenance and retention, please contact the Privacy Program at 773-834-9716 or hpo@uchicagomedicine.org

AI Scheming

We have mentioned before that a lot of our information is available online to the public. As examples:

- If you own a house, your name as an owner is public record and can be found by your home address. https://www.propertyrecord.com/property/v5
- In similar fashion if we give a speech at a public event, publish an article or book where our name and affiliated organization is used, folks can find out where we work, what our position is and make informative guesses regarding who our peers are (LinkedIn is a great place for that).

So how are scammers and cybercriminals using this information with AI?

AI Scamming

AI voice scams are becoming more and more popular with cybercriminals. As a growing threat, cybercriminals use voice cloning tools to impersonate anyone from celebrities to our loved ones. By creating voice clones from online sources, they can trick us into giving them money or information with familiar voices.

- First, they put and two together of the above information and make inferences based on publicly available information.

- Next, we may get calls over time of someone asking for information like names, birthdates, social security numbers, and credit card information.
- Once enough information is captured, there are many free and paid for AI generated voice services where they upload any captured audio and have AI clone the sampling.
    - With AI you can either type a sentence and have AI read it or speak the sentence in real time and AI disguises your voice into the intended voice.

Cybercriminals are going as far as to enact out of this world sophisticated extortion tactics such as a kidnapping scenario where they have an urgent familiar voice asking the recipient to pay money for a ransom among other such tactics.

How phone scammers are using AI to imitate voices - YouTube

AI can replicate voices in high-tech phone call scams, FTC warns - YouTube

New warning of AI voice clone scam | GMA - YouTube

How to protect yourself:

- Always verify the number that is calling you.
- Verify the identity of a caller by asking them questions where only they would know the answers.
- Come up with a code only they would know and have them never give out that code.
- Never act too quickly on urgent messages or calls that request a decision based on immediate monetary payment.

Other AI Scams to Watch Out For

- **Deep Fake Video**– Is a fake video that uses artificial intelligence to manipulate the appearance and voice of real people. There are many apps and online tools that can make a deepfake video, such as SwapFace, Reface, Jiggy, Impressions, and more. Deepfake videos can be used and have been used for various purposes some of which are: replacing actors, used in fraud schemes, used in blackmail schemes, and defamation.

This is not Morgan Freeman - A look behind the Deepfake Singularity - YouTube

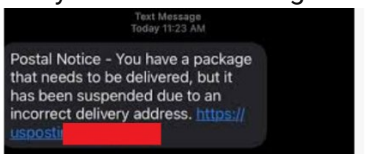
Deepfake of Zelenskyy Tells Ukrainian Troops to 'Surrender' - YouTube

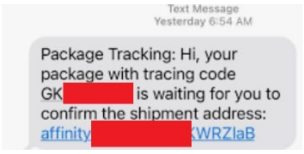
They can be created with deep learning software that can swap faces, change expressions, or synthesize speech from online sources. Deepfake videos can be hard to detect, but there are some clues to look for, such as unnatural movements, blurry edges, or mismatched audio.

- **Enhanced versions of old scams -** AI has been helping a lot of scammers correct their grammar on phishing e-mail messages, websites, advertisements, etc. Making it easier for them to create enhanced and convincing content to lure in victims.

Here is a listing of items to watch out for and tips to avoid falling for them:

- **Fake websites and ads:** Be wary of the legitimacy of websites you are visiting. Be wary of clicking on links and popups. If a website requests that you download and install software on to your system because you have something outdate, it is a scam!





- **Fake shipping notifications:** Shipping notices to your phone, e-mail or house are becoming a staple where notifications state that an item you ordered may not arrive due to your credit card being declined. Never reply directly to these notices. If you believe the notice may be accurate go directly to a vendor's website and contact them at the number they provide.
- **Fake surveys and charities:** Some scammers create fake surveys or charities that promise rewards, prizes, or tax deductions in exchange for your participation or donation. They may ask you to provide your personal or financial information, or to pay a fee or a tax upfront. To avoid these scams, always research the source and legitimacy of the survey or charity, and never give out your information or money to unverified or unsolicited requests. If you want to participate in a survey or donate to a charity, look for reputable and registered ones, and use secure and traceable payment methods. Be careful of emotional appeals or urgent deadlines that pressure you.

- **Use a credit card instead of a debit card:** When shopping online or in person, it is safer to use a credit card instead of a debit card. This is because credit cards offer more protection and security than debit cards and limit your liability in case of fraud or theft. Credit cards also have features such as chargebacks, refunds, or rewards that can help you recover your money or dispute a transaction. Debit cards, on the other hand, are linked directly to your bank account, and can expose you to more risks and losses if your card or information is compromised. If you use a debit card, make sure to monitor your

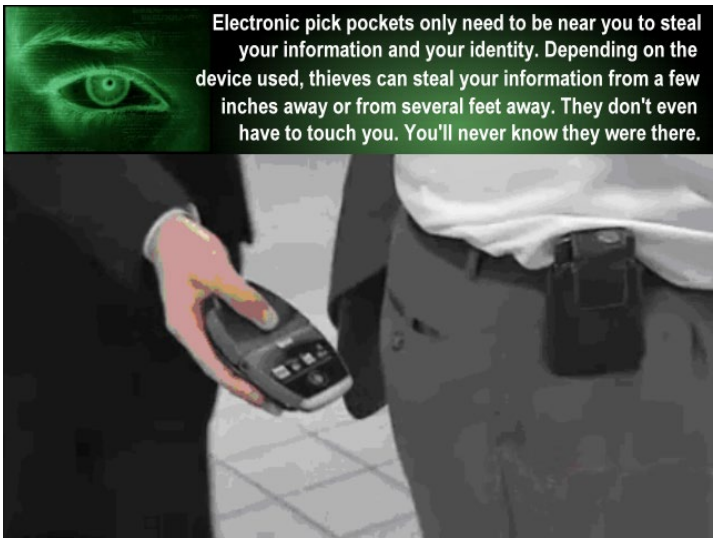
account balance and activity, and set up alerts or notifications for any unusual or large transactions.

- **If someone asks you to pay with crypto, a prepaid debit card, or a gift card, this is a red flag that it is a scam:** Some scammers ask you to pay with crypto, a prepaid debit card, or a gift card, because these are untraceable and irreversible payment methods that make it hard for you to get your money back or report the scam. They may claim that these are the only or the best options available, or that they offer discounts or incentives for using them. To avoid these scams, never agree to pay with these methods, and always use secure and traceable payment methods, such as credit cards, PayPal, or bank transfers. Also, be skeptical of any requests that ask you to pay upfront, or that involve sending money to someone you don't know or trust.

Physical Protections - Protecting Your Wallet/Purse, and Phone

Avoid Crowded Areas:

Be aware of the risk of electronic pickpocketing. Electronic pickpocketing is when someone uses a device to scan and steal card information from a distance, without touching your card or wallet. This can happen if your card has a chip or a contactless feature that allows you to pay by tapping your card or phone on a terminal. While these features are convenient and secure, they can also be exploited by thieves who have the right equipment and software. Credit cards require a few authentication mechanisms to be used effectively online (CVV Number – the 3-digit code at the back of the card, name on the card, address, etc...) but that is not to say it can't be used passively in some businesses that don't require it.



- **RFID protection:** RFID stands for radio frequency identification, and it is a technology that allows some credit cards and phones to be read wirelessly by a scanner or a reader. Some scammers use devices that can scan or skim your credit card information or connect to your phone from a distance and use it to make fraudulent purchases or transactions. To avoid these scams, RFID protection can help. Special wallets, sleeves, or cases that block the radio signals from reaching your cards exist and they are not pricey.

Never feel embarrassed or ashamed if you fall for a scam. We are here to help when needed. There is also the consumer protection division which can be contacted here:

ReportFraud.ftc.gov

Or as per out webinar during cybersecurity awareness month with the U.S. Secret Service, you can contact Joseph.kefer@usss.dhs.gov Phone:415-264-3763

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 .