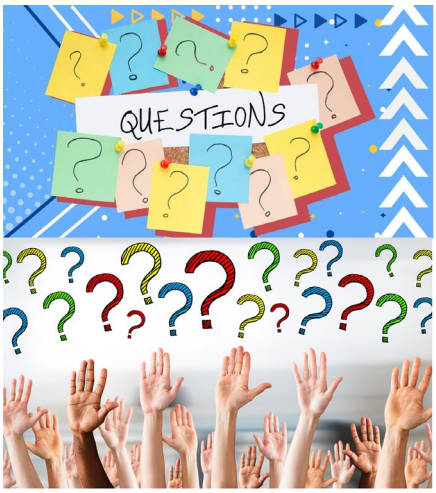
THE UNIVERSITY OF CHICAGO | Biological Sciences Division Information Security Office

April 2024

Cybersecurity Awareness Newsletter

Protecting yourself and information from cybersecurity threats.

This month we've compiled 5 inquiries that were sent to the BSD Information Security Office. These questions mirror the concerns, challenges, and curiosities that people have encountered in the realm of information security. Our goal is to empower individuals with the knowledge needed to navigate these issues with confidence, guidance, and appropriate caution. We hope that our responses will offer further insight and enhance your understanding of information security. After the Q&A, our intern gives his insight into cyber security from the student perspective. Please drop us a comment at security@bsd.uchicago.edu and let us know how he did.



Question 1:

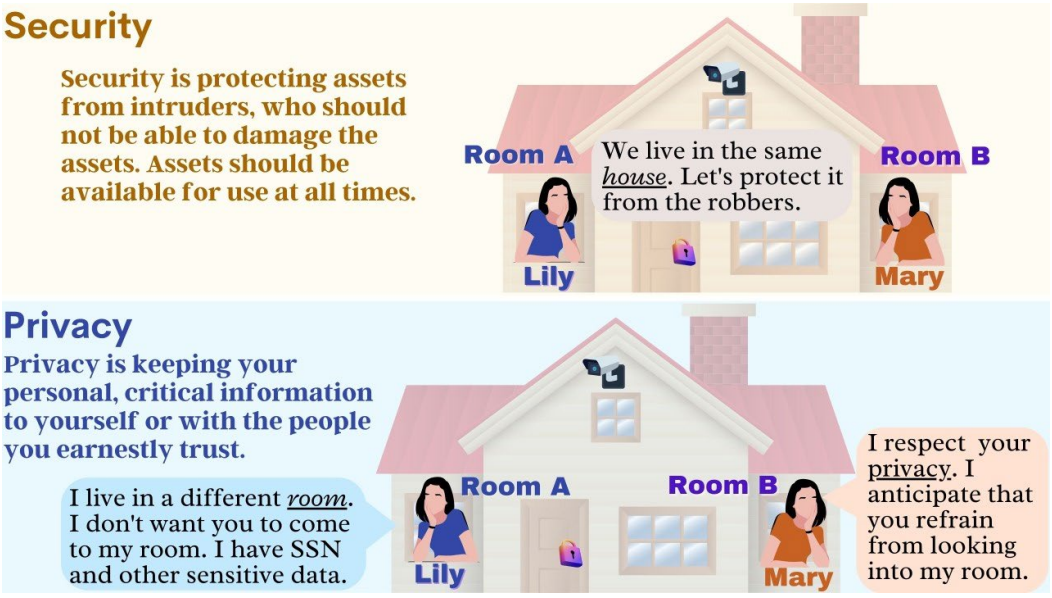
When using a credit card online, should we be using the Incognito feature in our web browser to make purchases?

Answer 1:

The Incognito mode in a web browser primarily serves as a privacy tool, not a security feature. Its main function is to prevent the storage of browser history, cookies, website data, and autofill information. For instance, if you're using a shared computer to enter credit card details, activating Incognito mode ensures the browser doesn't save this information. This prevents autofill suggestions from appearing to the next user, provided you close your session

completely. It is important to note that Incognito mode doesn't secure your credit card information within the browser. The security of your data relies on the measures implemented by the website you're using.

There are two key concepts are at play here that are often confused for one another: Cyber Security and Cyber Privacy. While they are interrelated, they are distinct concepts that are often misunderstood in the realm of computing. Cyber Security focuses on protecting data from unauthorized access, while Cyber Privacy is about controlling what data is collected and how it's used. Incognito mode primarily enhances your Cyber Privacy.

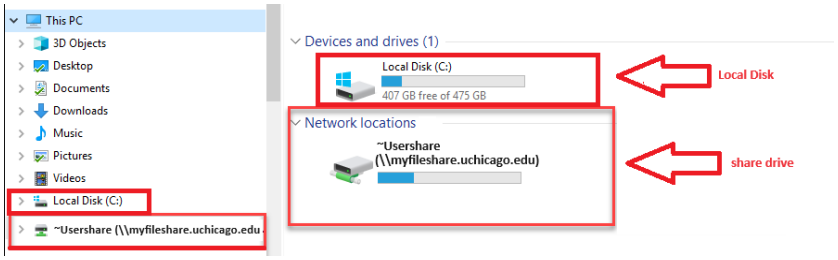


Question 2:

Why is it important to place data on a shared drive instead of on the desktop directly?

Answer 2:

The primary reason to store data on a shared drive is its regular backup feature, which ensures accessibility from various systems, providing a safety net in case of a hardware failure on your local system. A shared drive typically offers more disk space and enhanced security controls, such as stricter access controls and firewall rules. In contrast, data stored on a desktop can be more susceptible to threats.



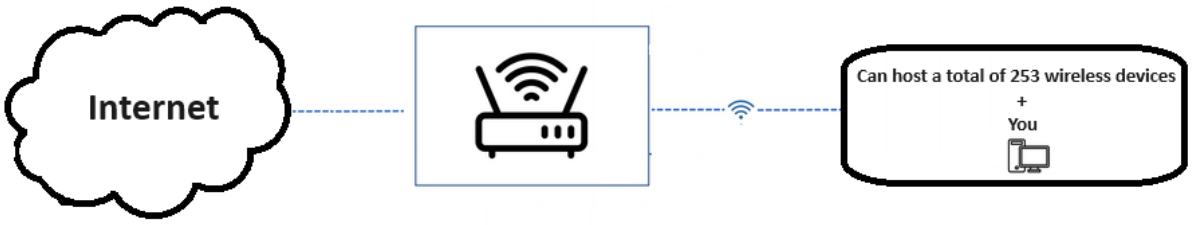
Question 3:

How can I stay safe while using public Wi-Fi?

Answer 3:

Here are 7 ways that can help you stay safe on a public Wi-Fi:

- Use a Virtual Private Network (VPN): A VPN encrypts your internet connection, making it harder for others to intercept and view your data.
- Visit Secure Websites: Ensure the websites you visit use HTTPS, which encrypts the data between your device and the website.
- Turn Off Sharing: Disable file and printer sharing on your device to prevent unauthorized access to your files.
- Keep Your Device Updated: Regularly update your device's operating system and applications to ensure you have the latest security patches.
- Use Antivirus Software: Keep your device protected with up-to-date antivirus software.
- Avoid Sensitive Transactions: Try to avoid conducting sensitive transactions, like online banking or shopping, on public Wi-Fi.
- Forget the Network After Use: Make sure your device forgets the network after use to prevent automatic reconnection in the future.



Question 4:

What are ghost calls?

Answer 4:

A **Ghost call**, also known as a **Phantom call**, is typically done by an automated dialing system often used by telemarketers, scammers and robocallers which can spoof (impersonate) a phone number. This is like e-mail phishing in that it uses the tactic of

expecting you to answer or call back a missed call notification. The phone number you see on your phone from the missed call is usually a random number of either a valid or an invalid phone number which may or may not be tied to a malicious user. The creation of a missed call on your phone is done on purpose since the automated dialing typically generates one ring on your phone and immediately terminates the call. If you call that number back, which is what they expect you to do, or you answer the call before the ring ends the following can occur:

- You can hear a series of beeps or silence letting the system that just autodialed you know you exist. This existence of a live person is then sold online to companies or scammers and will lead to more aggressive calls where they expect you to answer.
- The call has a live person that answers and tries to manipulate you into giving up sensitive information for an item or service (it can be a vishing tactic).
- You can be charged for a long-distance call connected to the sammer and they will generate money from a small percentage of the call. Calls like this are usually done in bulk.

Unfortunately, spoofing a phone number is not illegal unless there was malicious intent behind it. The system owner may claim a glitch which may or may not lead to litigation.

To help reduce and mitigate these type of phone calls you can register your phone number in the National Do Not Call Registry: https://www.donotcall.gov/. However, this is not a 100% fool proof solution since the FTC does have exemptions to their rules: https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#exemptions. Not all businesses are based in the United States and have to follow these rules. That being said, the Telephone Consumer Protection Act (TCPA) can be used to sue companies that violate the **do not call** requests and can act as a deterrent for those times when you have a telemarketer that just won't quit calling.

Question 5:

How can I help my elder family members from falling victims to scams?

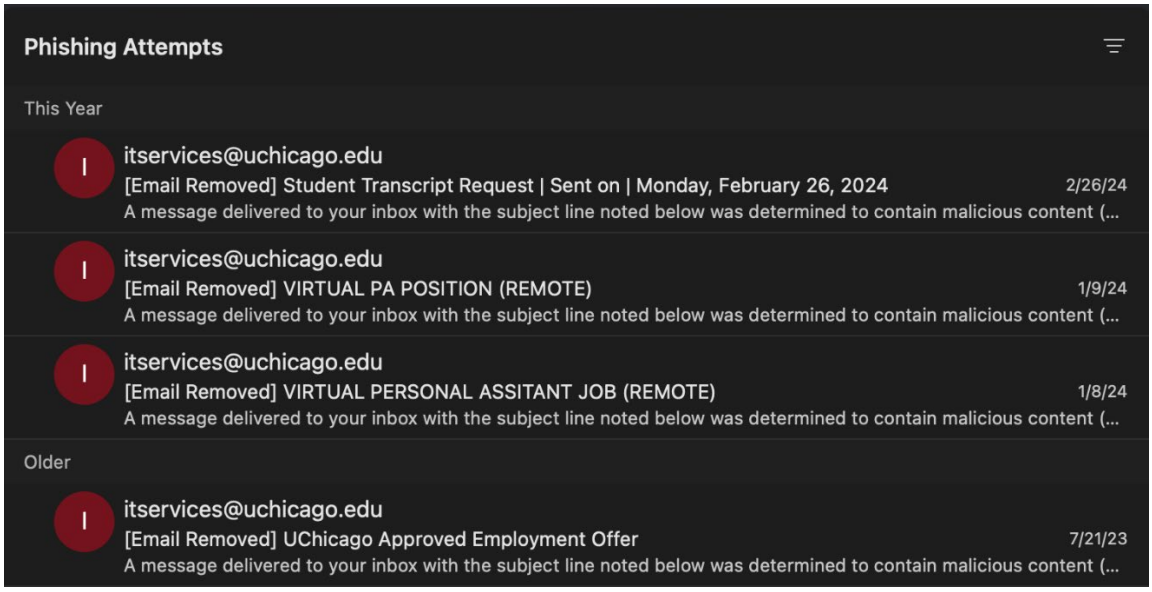
Answer 5:

Communication, Education, and Vigilance. In that order. As we get older it is not uncommon for us to find ourselves gradually falling out of the rapid pace in technological advancements. What was once intuitive may feel overwhelming and unfamiliar. While it is not uncommon to feel frustrated and embarrassed by a 6-year-old who can navigate a smart phone better than most adults, that same technology creates a bridge between the generations to unlock countless of opportunities and overcome the dangers that exist in the digital landscape for both elderly and young'ns alike as well as enhance our daily lives.

Nik's Corner!

Hi, I'm Nikola Bilaver, an undergraduate 3rd year student at the University of Chicago, and I am interning at the BSD Information Security Office! Here, I will share my insights on security topics from my perspective as a student, which might be helpful to you!

This first topic will discuss phishing, and the ways a malicious sender might personally target you. It is easy to think that these malicious senders are just sending generalized emails to as wide an audience as possible, to 'cast a wide net' to align with the fishing analogy. While this isn't an inaccurate analogy, thinking of phishing and spam as wide nets can make one think that they aren't targeted towards them, which is not always the case. For instance, many of the spam and phishing emails I receive as a student are targeted specifically to college students.



Here are some emails that were removed from my inbox. Notice the topics of these emails were mainly with jobs suited to students or a false request for my transcript.

While it is often easy to think: "There's no way that anyone could fall for something that obvious!" When thinking of a generalized spam email, the targeted nature of these emails can make them more dangerous than expected. There is the potential to be attacked with personally tailored emails for University employees and organizations, an attack known as 'spear phishing'. For instance, an attacker might create an email with the same name as a coworker, making one more likely to trust a link or attachment within the email. While attacks of this nature are rarer due to the effort required to personalize them, they can be highly effective. This highlights the importance checking for red flags in any incoming email, such as incorrect email addresses, whether it is asking for sensitive information, or if hovering over a link gives a URL that is expected.

The perception of phishing with a wide net vs. being specifically targeted in spear phishing.

Hopefully this has highlighted an aspect of phishing that you might have thought about before, and when you receive an email that seems a bit too good to be true, it can help you catch the attempt and report it.

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 .