Published Date(s): 1/10/2024
Title: Spider Secure New Year Resolutions
Message: Happy New Year from the Information Services Security Team! As we enter the new year, we wanted to share some of our Spider Secure resolutions. First, we want to continue expanding the use of Duo multi-factor authentication (MFA) across all platforms. MFA is proven to make you less vulnerable to being compromised. Second, we want to share and educate users on data security for ChatGPT and other Generative AI technologies at UR. We hope to grow the awareness of safely using these new technologies as they become more integrated within the UR community. And our final resolution is to continue creating awareness and engaging opportunities to grow your understanding of what it means to be Spider Secure at UR. We want you to know how to best protect yourself while online, know how to identify and report suspicious cybersecurity activity, and how to avoid being a victim of cybercrime.
Website Link: https://is.richmond.edu/infosec/index.html

Published Date(s): 1/17/2024
Title: Data Privacy Matters
Message: All your online activity generates a trail of data. Websites, apps, and services collect data on your behaviors, interests, and purchases. Sometimes, this includes personal data, like your Social Security (SSN) or driver's license numbers. It can even include data about your physical self, like health data – think about how a smartwatch counts and records how many steps you take. While it's true that you cannot control how each byte of data about you and your family is shared and processed, you are not helpless! In many cases, you can control how your data is shared. You can start by updating your privacy settings using the provided website, maintained by the National Cyber Security Alliance (NCSA), that provides useful information for managing privacy settings for many common applications and services. Remember, your data is precious and valuable, and you deserve to be selective about who you share it with!
Website Link: https://staysafeonline.org/

Published Date(s): 1/24/2024
Title: Data Privacy Week
Message: The National Cybersecurity Alliance (NCSA) has declared this year’s Data Privacy Week is from January 21, 2024, to January 27, 2024. Your data is collected everyday — from your computer, smartphone, smartwatch, and pretty much every other internet-connected device you own! Many companies have the opportunity to monitor your data, often in the process of providing services, but some may try to sell that data for profit as well. Your data may even be used to train Artificial Intelligence! You often have some control when it comes to how this data is collected, shared, and sold, though. The goal of Data Privacy Week is to spread awareness about online privacy and how you can protect your data from potentially being used in a manner you do not agree with. Data privacy should be a one of your top priorities in our ever more complex technical world.
Website Link: https://is.richmond.edu/infosec/dataprivacyday/index.html

Published Date(s): 1/26/2024
Title: MFA or be Breached
Message: 26 billion records!!! A supermassive Mother of All Breaches (MOAB for short) was recently discovered by cybersecurity researchers. Though the leak contained mostly information from past data breaches, there is evidence some of the breached information is relatively new. Malicious cyber actors are quick to use these leaks to attempt to gain unauthorized access to your accounts. By using Multifactor Authentication (MFA), you can reduce your likelihood of being hacked. Duo is the official MFA app used at UR. MFA helps prevent unauthorized users from gaining access to your accounts, even if your password has been stolen or exposed. It provides extra security step by confirming your identity when you log in, by either requiring you to acknowledge a Duo Push or enter a Duo Mobile Passcode. With 26 billion compromised records floating around on the internet, use MFA to reduce the chance that a security breach will ruin your day!
Website Link: https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/#google_vignette

Published Date(s): 1/31/2024
Title: Stop. Think. Connect.
Message: While the Internet is a great place to swap pictures and make weekend plans, keep in mind that cyber criminals are lurking; even your former and future employers are finding out about you through social media. Cyber criminals can use information provided from your social media profile, such as your birthday, hobbies, and interests to guess the answers to security questions on your accounts or impersonate a trusted friend. What you say and do online is visible to others, and it cannot be erased. Before posting STOP for a moment to THINK is this information something that could be used harmfully against me. Furthermore, check to see if your privacy restrictions are set to the audience, you want knowing your information, such as your close friends. Once you determine if the information is something you still want to share then continue to CONNECT with your online community.
Website Link: https://www.cisa.gov/sites/default/files/publications/Undergraduate%2520Student%2520Presentation.pdf