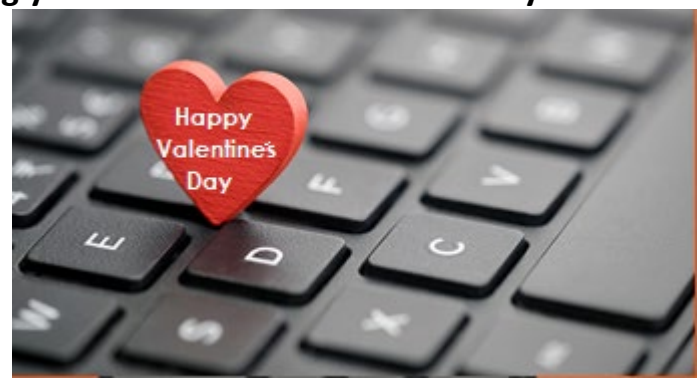
THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

February 2023

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats



This month Valentine's Day is right around the corner which means the internet traffic relating to online dating sites and all sorts of gift ideas for loved ones is in full swing. This is the perfect opportunity for cyber hackers to find vulnerable heart strings to pull. This month we want to dive into Valentine's Day cyber threats and what you can do to protect yourself from these cyber threats.

It's well known that people online aren't always who they appear to be. However, tens of thousands of internet users fall victim to online romance scams each year, and it can happen to anyone. These scams can be incredibly convincing and are increasingly found across dating sites and social media platforms. Bad actors are very good at appealing to victims' emotions with the intention of stealing large sums of money and personal information. Luckily, there are ways to identify a scam and protect yourself online.

TIPS

Ask yourself the following questions:

1. How could a scammer target me?
2. Why would a scammer choose to target me?
3. What information could a scammer use to target me?

The Red Flags:

1) They send you an e-mail expecting you to click on a link or download a file.
2) Urgent requests for money that can stem from:
    a. A plane ticket
    b. Pre-loaded gift cards
    c. Wire transfer
    d. Medical expenses
3) Claim to be overseas or be in the military.
4) The relationship is moving fast.
5) They try to get you to move to a different media platform.
6) They request that you install software.
7) They will break promises or other engagements and expect you to respond to that negativity.

Staying Safe

CHECK ACCOUNT SETTINGS

Consider setting your social media profiles to “private.” This will make it harder for scammers to target and communicate with you. A public profile will make it easy for scammers to find your profile and learn about you through old posts and photos.

THINK BEFORE YOU ACT

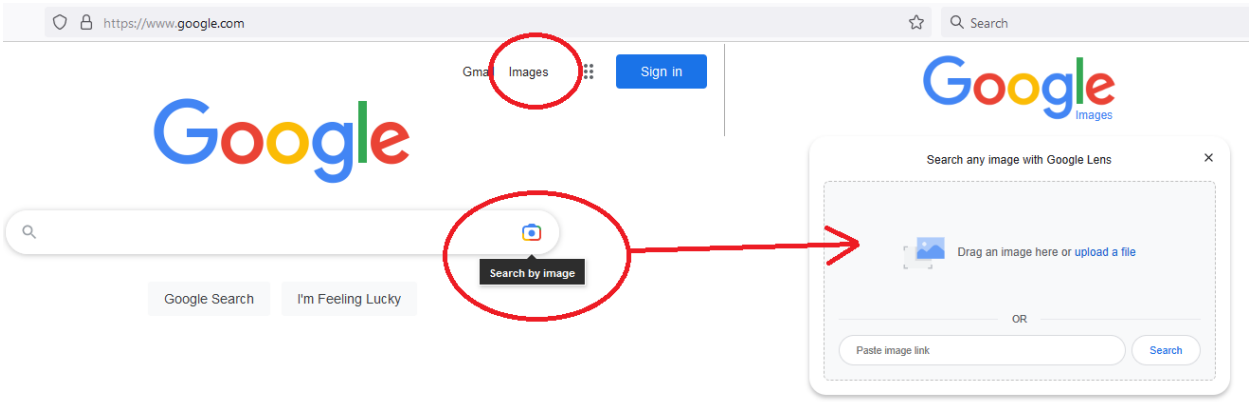
Be wary of communications that push you for immediate action or ask for personal information. Never share personal information through email, especially if you do not know the sender.

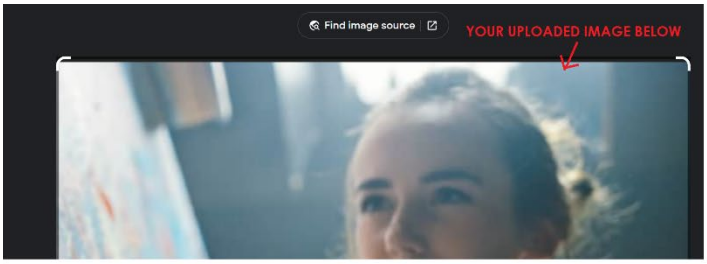
SHARE WITH CARE

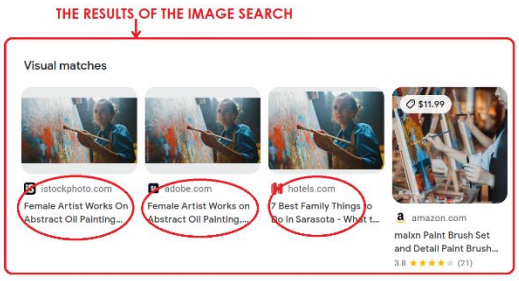
Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others. Consider creating an alternate persona that you use for online profiles to limit how much of your own personal information you share.

Reverse Image Searching

If you are unsure if you're being scammed, do a reverse image search of the potential scammer's profile picture. You may see that image belongs to a completely different person or has been affiliated with different online identities.







Some contexts

1) There is a lot of public information about everyone available on the internet, so don't let public information fool you.
    a. There have been many businesses where customer information has been harvested by cyber criminals.
    b. Public and stolen information can be used to lure folks into clicking on malicious links or installing software.
2) Websites are spoofed often, meaning a fake website can be made to look like a legitimate website where it can be nearly impossible to tell a legitimate web site vs a fake web site without closer inspection.
3) Don't fall for phishing scams. Phishing scams are still the #1 cause of cyber related data breaches.

If you feel that you have been scammed at the institution, please reach out to security@bsd.uchicago.edu and we will help you take the necessary steps to secure your account and data. It should be noted that we at the BSD Information Security office **do not judge** individuals. We are here to help protect you from cybercrime.

Public Service Announcement

It is important to understand that different generations of individuals react differently to scams and those that lack experience with technology makes them susceptible. It is well known that cyber criminals target older age groups since they have a more significant amount of savings, making them attractive targets. These scams can result in significant financial losses, emotional distress, and loss of self-esteem for the victim. It can be too embarrassing to report a scam, so for our readers, I leave you with an action item: It is important for families and caretakers to educate and protect our older generation of individuals from these types of harmful and deceitful scams to prevent financial and emotional harm.

DID YOU KNOW?

People who said they were ages 40 to 69 reported losing money to romance scams at the highest rates – more than twice the rate of people in their 20s. At the same time, people 70 and over reported the highest individual median losses at $10,000. (FTC)

Helping others by educating and showing kindness can bring happiness and fulfillment to both the giver and the recipient, and it's a wonderful way to celebrate Valentine's Day. By lending a hand to those in need, you can demonstrate love, compassion, and generosity, and make a positive impact in someone's life.

Hope you have a wonderful February!

-BSD Information Security Office