Securing Your World: Tips in Times of Transition

Mashup – January 17, 2024

Agenda

- Introduction
- Background on cybercriminal activity
- Scenario
  - Lessons Learned
- How can you help reduce the risk?
- Discussion / Questions

Con artists transition to cybercriminals

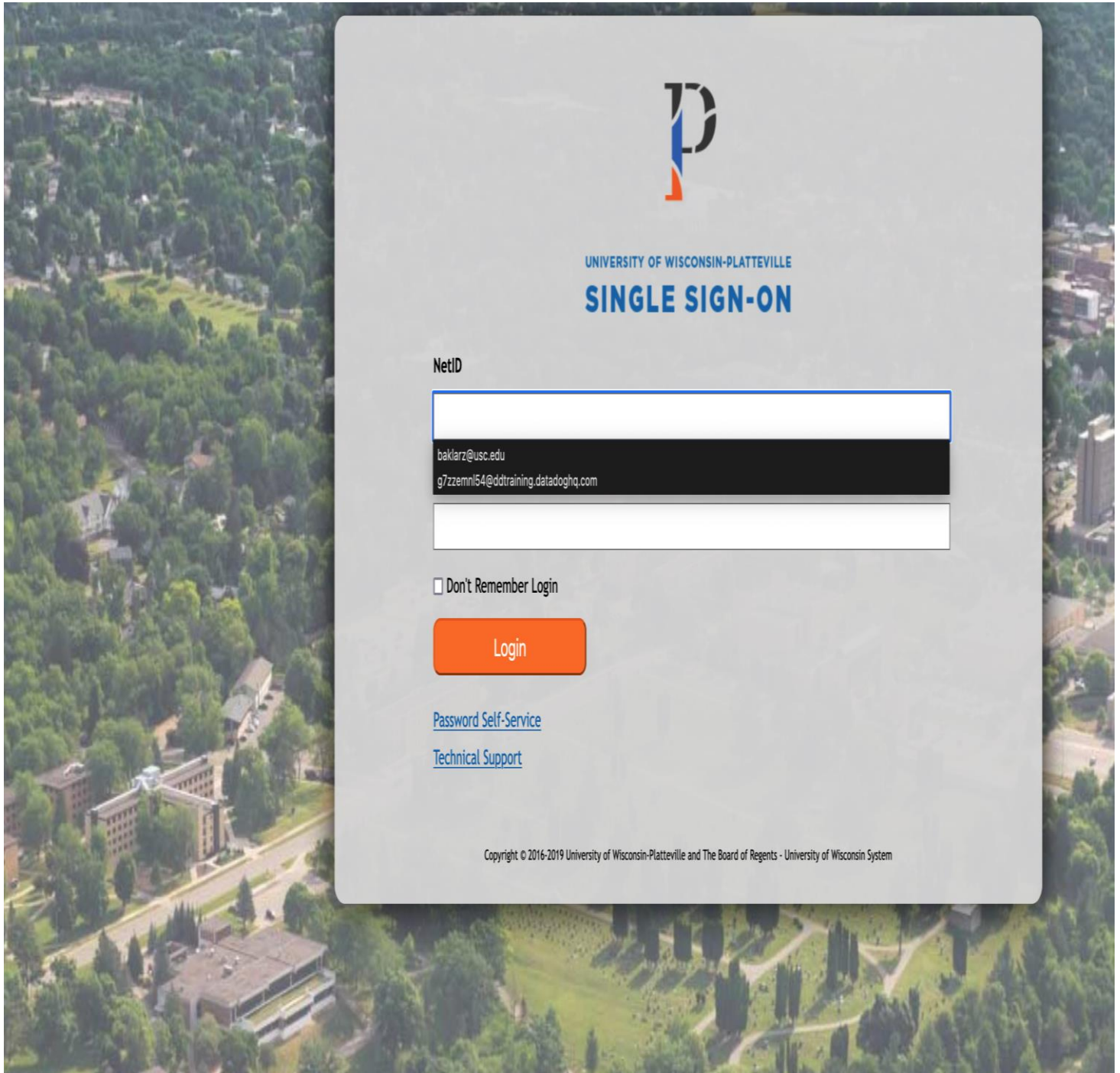
- Earliest recorded fraud was 300 BC
  - Merchant took a loan against cargo to be delivered but sank his own ship to keep the money
- Play off human emotions
- Leverage psychology and human behavior to their advantage
  - Stress and Anxiety
  - Fear, Uncertainty and Doubt
  - Urgency and Distraction
- Uptick in malicious activity during times of stress
  - Holidays
  - Loss
  - Natural Disasters, Pandemics, Unrest / War
  - Transition

Scams, threats, intimidation, social engineering, and other tactics

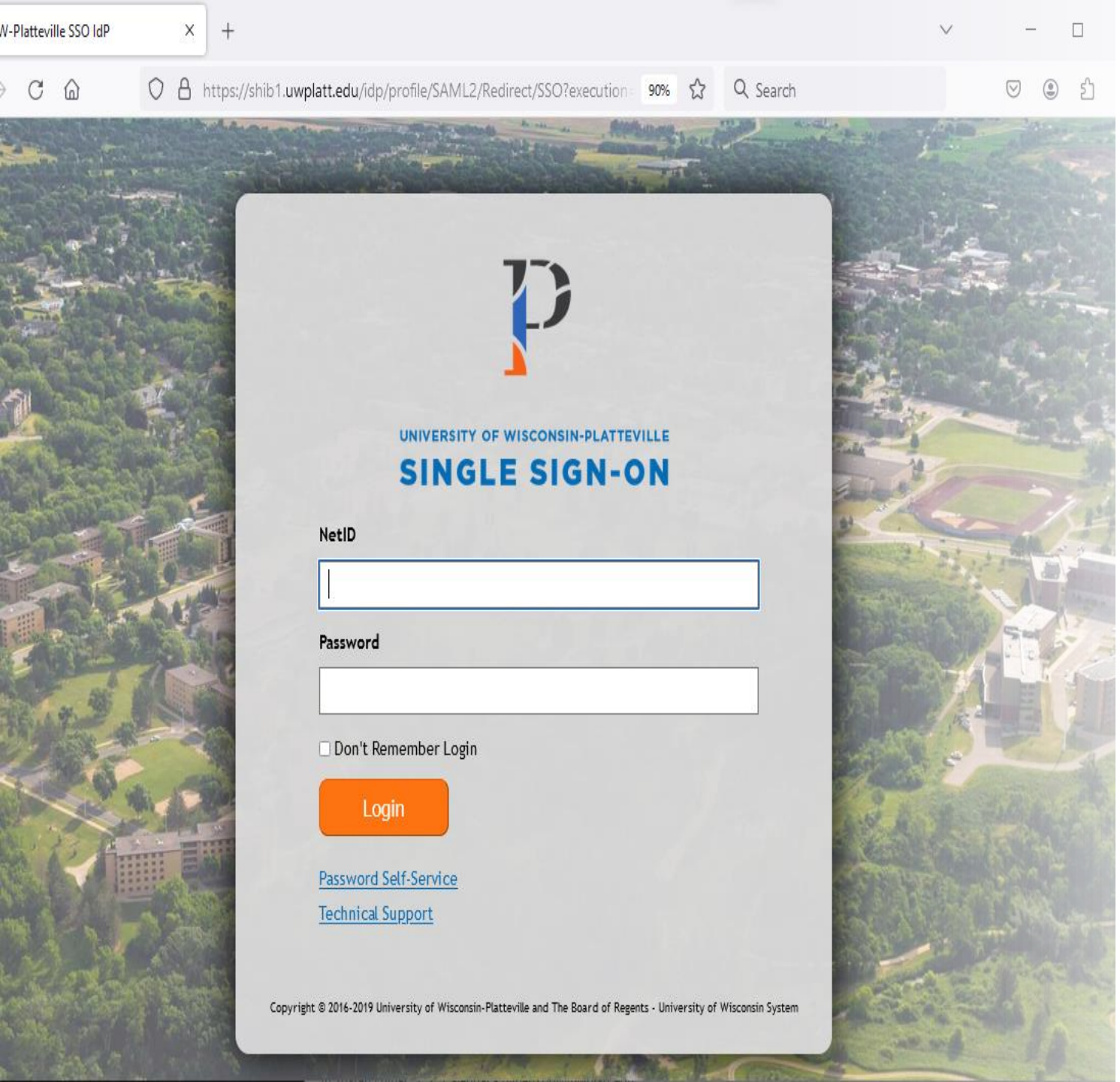
- Cybercrime is typically conducted for financial gain
- Cybercrime industry is worldwide, and very well organized
  - Ransomware as a Service, Phishing as a Service, selling stolen credentials and data, etc.
- Cybercriminals share ideas and methods, often resulting in “copycat” crimes
- Social Engineering continues to be very successful to gain access to data
- More difficult for the activity of the cybercriminal to be noticed if they access data using trusted credentials – e.g. steal an employee’s credentials and use that to access the data or systems.
  - Cybercriminals hiding in plain sight, and often attempt to cover their tracks to reduce the risk of being caught

Social Engineering and credential stealing

- Description of the phishing email
  - Tactics used – Urgency, Health concern (“Important Safety Notice”)
- What happened when the link was clicked
  - Malicious website, which was designed to appear similar to our UW-Platteville Single Sign on page, requested the recipient to log in
    - URL for the web page was NOT from uwplatt.edu
  - If the recipient entered their UW-Platteville userid and password, both were harvested by the cybercriminal.
  - Recipient was then prompted for their Duo credential. If the recipient responded, the cybercriminal was able to harvest the information and successfully log into systems AS THE ACCOUNT HOLDER
  - No additional web pages were displayed.
- Cybercriminal now had full knowledge of the account holder’s password, and control over the individual’s credentials
  - Use the credential to access system(s) and data, sell the credentials and harvested data, etc.



- The FAKE UW-Platteville Single Sign-on page.
- The domain is NOT from UW-Platteville (uwplatt.edu)
- The URL includes **https://[malicious.domain]/uwplatt.edu/**…..



- The REAL UW-Platteville Single Sign-on page.
- The domain IS from UW-Platteville (uwplatt.edu)
- Note the URL includes **https**://shib1.**uwplatt.edu**/…..

What data and systems can be accessed by compromised credentials?

- What systems and data does your account have access to read or modify?
  - Examples: Email, Teams, SharePoint, HRS, Parking, Zoom, password change, Duo profile, etc.
  - Student information, department information, financial information, etc.
- What type of information could the cybercriminal harvest and use to their advantage?
  - University information, student data, your personal information, research data, etc.

Why didn’t Duo protect the account?

- Multi-factored authentication:
  - Something you know (userID and password/passphrase)
  - Something you have (Duo app/token)
  - Something you are (Biometrics)
- Using multiple forms of authentication reduces the risk of cybercriminals stealing the account to access data.
  - The risk is reduced, NOT eliminated.
- Cybercriminals are able to use many methods to determine “something you know” (userID/password)
  - Guessing, using passwords that were identified during other breaches (Chegg, Facebook, LinkedIn, etc.), or by asking (social engineering, fake login pages, etc.)
- Cybercriminals use methods to gain access to “something you have”.
  - MFA fatigue – once the userid/password is known, keep attempting to sign in and hope the individual will accept the Duo prompt or enter their Duo code.

What can I do to help protect my account credentials and the data?

- For ALL incoming communication, VERIFY the source first, then determine the appropriate level of trust.
  - Email, text messages, phone calls, physical mailings, etc.
- When logging into a system, VERIFY the login page is from the correct and expected source prior to entering your credentials
  - VERIFY the URL of the login page, not just the appearance of the page
    - For single sign-on, the URL should include HTTPS://shib1.uwplatt.edu/
  - VERIFY the Duo prompt is from the trusted source to which you are currently attempted to authenticate.
    - If in doubt, do not accept the push notification or enter the Duo passcodes.
    - If you receive an unrecognized Duo request, it may be an indicator your password has been compromised. Consider changing your password and contact the Help Desk for additional assistance
- When you see something, say something
  - Report unusual account activity and suspicious communication, such as phishing messages to the Help Desk
  - Periodically review your email settings, registered Duo devices, etc.

How does this relate to times of transition?

- Cybercriminals can leverage times of transition to improve their social engineering tactics
  - Call and ask for information
    - Data, personal cell phone and/or email addresses, etc.
  - Craft targeted content to use in unsolicited incoming messages via email, SMS text, voicemail, etc.
- Change in roles
  - Verify the methods to log into and access the system(s).
  - Review access and authorization rules
- Increase awareness and report suspicious activity

Summary

- Cybercrime is increasing in frequency, and their tactics can evade detection by technology.
- The best defense is a good offense.
  - Being proactive will provide a strategic advantage when confronted by the threats from cybercriminals.
  - Protect your accounts
    - Use different and strong passwords for each account
    - VERIFY the login pages and Duo prompts prior to entering credentials or accepting a push notification.
  - VERIFY all incoming communication, then determine if it is safe to trust.
    - Stop and verify prior to responding or interacting with the incoming communication.
  - Trust your gut. If something seems a bit “off”, report it to the Help Desk.
- If you see something, say something
  - Help take a “byte” out of cybercrime by reporting suspicious activity
  - ITS Alerts
- The approach of constant vigilance combined with layers of strategic actions are designed to reduce your risk of compromise.

Discussion / Comments / Questions?

THANK YOU for your participation !!