Social Engineering

Reese Hatfield

Social Engineering

- No matter how secure your system is
- There is always a human factor

- Cannot ignore that people are often the weakest link
  - Not your way of storing data

Social Engineering

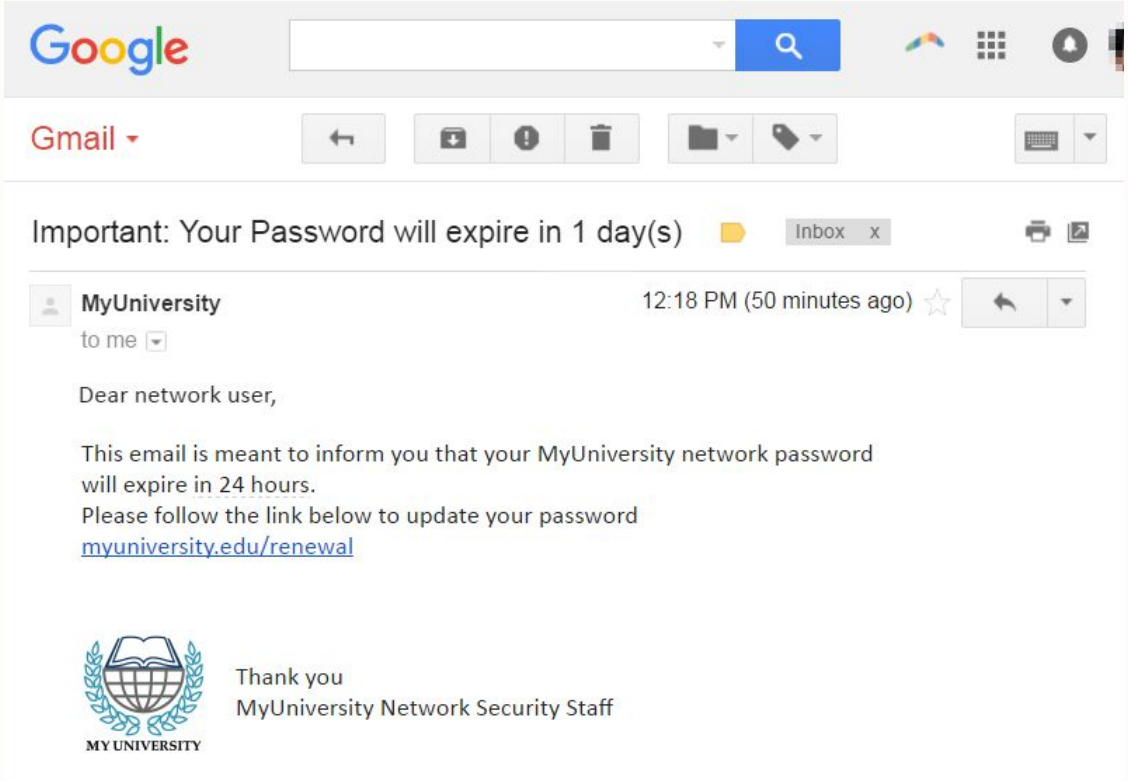
- Exploit Psychology
  - Human Behavior
  - Curiosity
- Techniques are used for several reasons
  - Scams
  - Data
  - Money

Social Engineering

- **Phishing**

- Message a user in some form
  - Email
  - Text
  - Phone
- Pretend to be legitimate

Social Engineering



Social Engineering

Email Scan Alerts (Phishing)

Recently there has been a large number of phishing attempts targeting Wright State University students, faculty, and staff. These attempts appear in the form of an email sent to a university inbox, and tries to get the user to "verify account information" by sending their CAMPUS username and password in an email, or clicking on a link within the email.

CaTS has developed this page to provide you with tips on how to keep your information safe from phishing attempts, and to alert you to any attempts you may see in your inbox. Please take a moment to review the "Points to Remember" section on the right for tips on how to protect your account information. Then, review the examples below showing the many recent scams targeting Wright State. If you receive an email that looks like any of these, do not reply to it or click on any of the links in the message.

If you have reviewed the information on this webpage and are still unsure as to the authenticity of an email you have received, please do not hesitate to contact the Help Desk at 937-775-4827 or 1-888-775-4827, or by email at helpdesk@wright.edu. We will help in any way we can to validate the email you've received.

Points to Remember

- CaTS will never ask you for your account information (username or password) in an email.
- If an email is difficult to read (poor grammar or wording), it is most likely a scam.
- If you receive an email about a problem with your account, do not click on any links or provide your username and password. Go directly to the site and log in.
- Do not follow any link in an email coming from an unknown source.
- Banks, credit unions, and other financial institutions will never ask for your account information in an email.

Social Engineering

- Detection
  - Grammatical errors
  - Fake urgency
  - “There’s a problem!”
  - Weird Addresses

Social Engineering

- Tend to target elderly
- As well as corporate figures

- Very general category of techniques
  - Not limited to any particular audience or strategy

Social Engineering

- **Advance Fee Scam**
- “Nigerian Prince” style scams

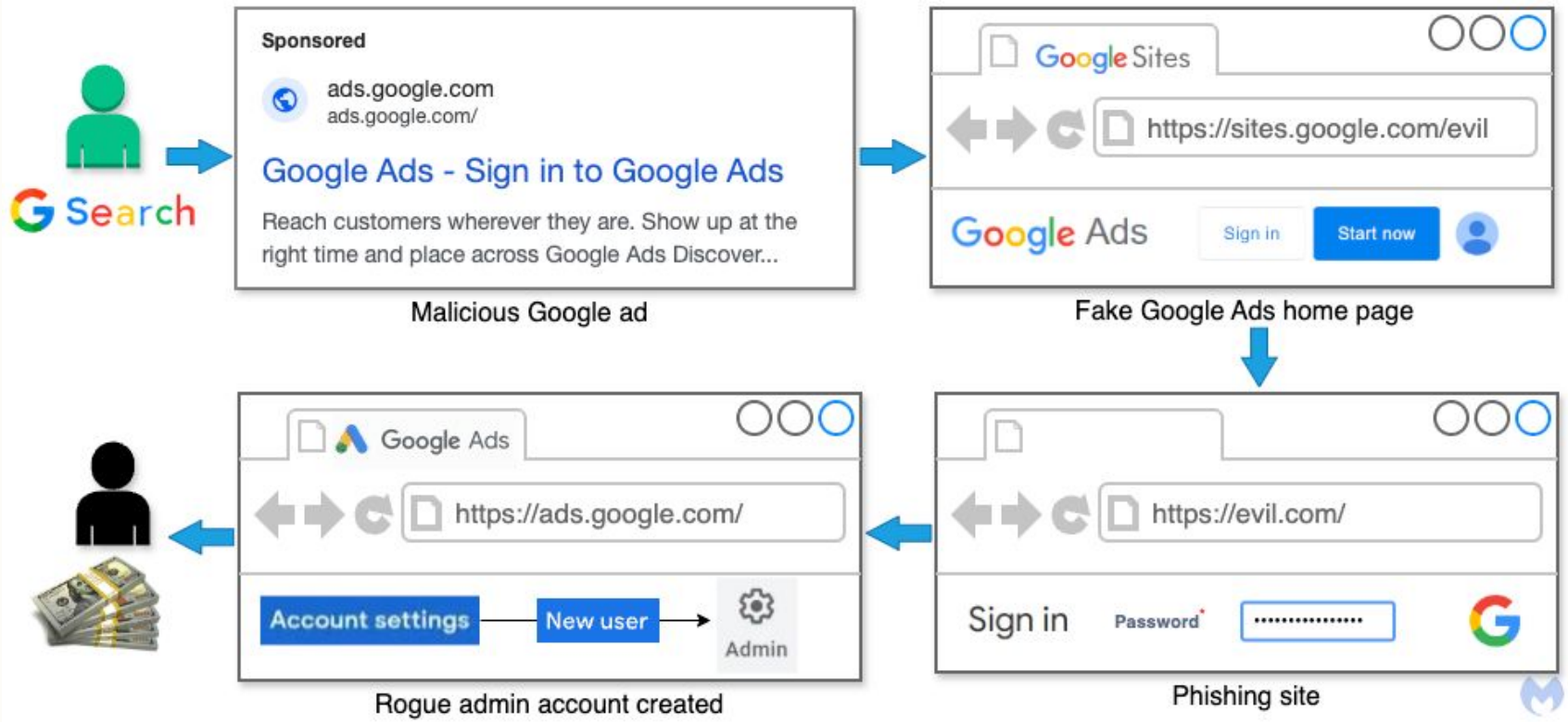
- Pretend to be someone with a lot of many
- “If you send me a little money, I’ll send a lot more”
- Bail out before money is sent

Social Engineering

- **Ad Phishing**
- Create a fake ad for a legitimate product

- User’s click on your ad instead
- Many directions you could go
- Large companies are bad about this, just too many ads to monitor

Social Engineering



Social Engineering

- **Baiting**
- Playings on human curiosity

- Leave removable media around
- Contains malware

Social Engineering

- University of Illinois
- Left about 300 drives out

- Almost all were taken
- A little less than half ran the files contained on them

Social Engineering

- **Pretexting**

- Invent a scenario
- “Pretext”
- Sense of urgency
- Get the user to divulge personal information
- Anecdote

Social Engineering

- **Tailgating**

- Physically impersonate someone
- Enter an office or warehouse, etc.

- Common: pretend to be maintenance or main person

Social Engineering

Social Engineering

- **Scareware**

- Scary and intimidating malware
- You must do this or else

Policy and Agreements

- How can we prevent social engineering failures?

- Robust security policy for internal employees
- (possibly for end users)

Policy and Agreements

- Internal Security Policy

- Usually broken down into specific
- Acceptable use policy
- Solid security trainings

- Define policies of use for employees and **end users**