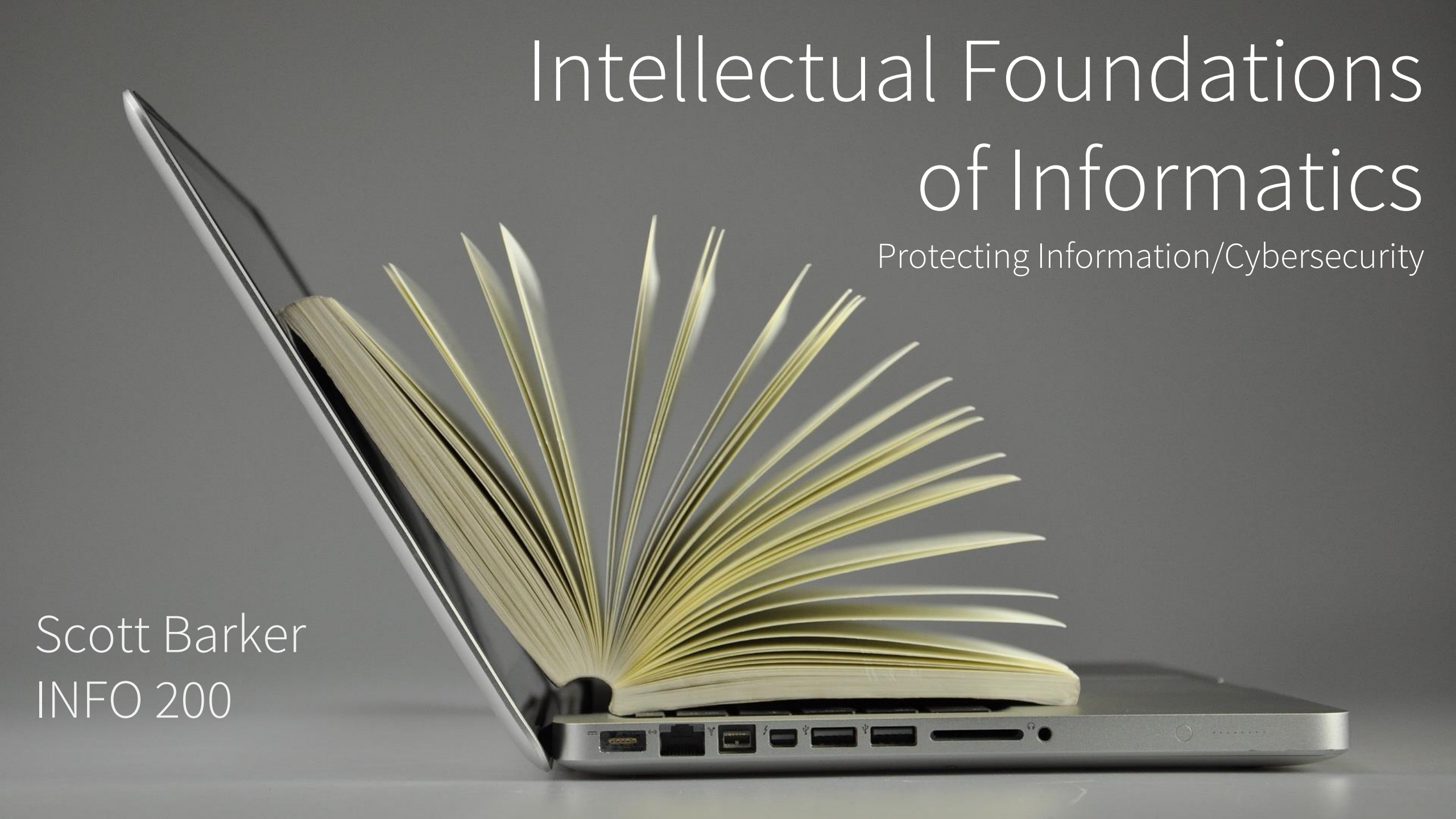
Intellectual Foundations of Informatics

Protecting Information/Cybersecurity



Scott Barker

INFO 200

- Protecting information is primarily about controlling who or what is able to access that information.
- It also is about ensuring information is recoverable if lost (e.g. storage failure or disaster)
- and properly retained in case it is needed in the future.
- Government and industry regulations (such as FERPA, HIPAA) impose disclosure requirements on certain types of information (e.g. education, and health records)
- Other regulations impose records retention requirements for varying periods of time (e.g. UW Retention Schedules), tax documents
- We must protect data at-rest as well as data in-flight

Examples of personal life information we might want to protect…

- Grades in school
- Information about personal relationships
- A past experience that is embarrassing
- Financial/bank/credit card information
- Personal identifiers such as SS #, student number, login info
- Family, national origin, immigration status
- Email, text messages, phone or video conversations
- Digital photos, Online videos we watched
- Files/documents on our computer or other device
- Internet search history, books that we read from the library

Examples of information that organizations or companies might need or want to protect

- Product “secrets” – specs, how something is made, product ingredients
- Research on new products or services in development, research on their competitors
- Unflattering news, poor sales or profit projections
- Communications – internal or external
  - Email, text messages, phone calls, videoconferences
- Customer data – e.g. health records, shopping history, credit cards, “friends”
- Photos
- Files/documents – print and digital
- Databases
- Systems – e.g. websites, “line of business systems” that are on-prem or in the cloud

One of the primary reasons we need to protect and secure information is that risk is present.

What is risk?

Risks are threats, actions, positive or negative events, gaps or variability that creates uncertainty or that may cause damage to us, our organization, or others

Damage could be financial, physical, personal, loss of reputation, sickness, death, others…

Everyone takes risks

- To be alive is to take risks. We take risks every single day. Driving a car, crossing the street, not doing our homework, carrying our laptop, going out during Coronavirus.

- Risks exist at
  - Home
  - Work or school
  - On the road
  - Online

- Ignoring certain risks can be expensive, can you give an example?

- We can identify risks in advance and take reasonable precautions that may reduce the level of risk

  In enterprises/companies this is known as “Risk Management” and many companies hire “Risk Managers” to proactively manage, monitor, and report on risk

Access Control

- To protect information we must control who has access **and** precisely what rights or permissions they have to that information

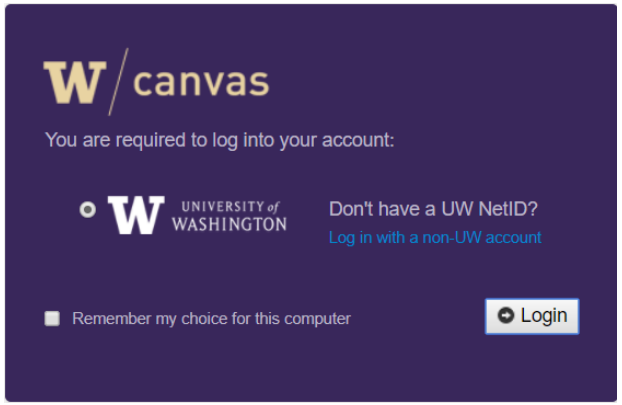
- For IT, these are broken into two distinct and separate pieces

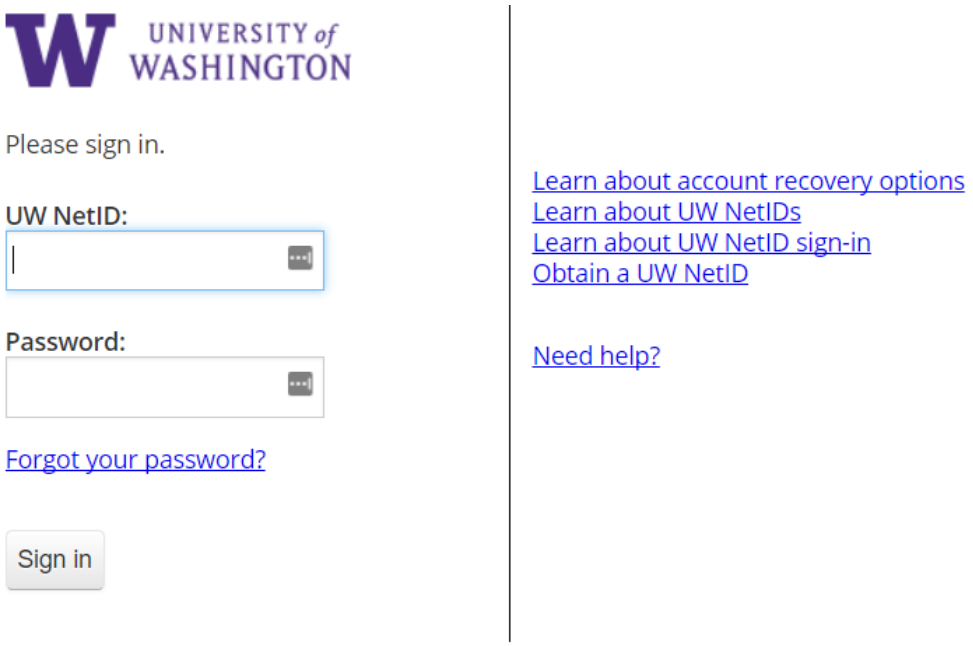
  – Authentication, verifying who you are

  – Authorization, verifying what you can do

Authentication

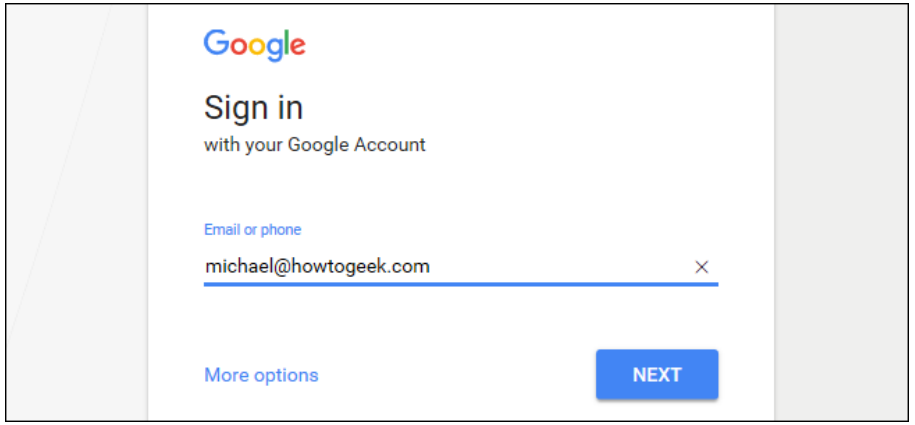
- The process of verifying a claim of identity by some entity
- Three primary ways to authenticate
  - With something you know (like a userid/password), most common
  - With something you have (e.g. your phone)
  - With something you are (biometric data)
- For example I can claim that I am “Scott Barker” when I go to the course Canvas website
- To prove my claim, an authentication system asks that I provide credentials using “something I know”
- By providing a valid UW NetID that I know, with a matching password that I know, I am “authenticated” and can use the system





Common methods of authenticating to systems

- Userid and password (something you know)
  - On many systems the userid is an email address
- Biometrics (something you are), note there are concerns about some of these technologies
  - Finger-print readers, Touch ID
  - Facial recognition - “Windows 10 Hello”, Apple iPhone Face ID
  - Voice recognition
  - Retina scan
- Smart-cards, Yubi keys, your smart phone (something you have)



Passwords

- We use them everyday, but there are many problems
  - Passwords can be guessed – let's play a password guessing game!

What if we played a guess the password game?

Round 1 – my password is a single number between 0 and 9. Guess!

Round 2 – my password can be any two numbers between 0 and 9. Guess!

Round 3 – my password can be 20 letters, numbers, or any symbol on a standard keyboard. Guess…yikes!

Length matters. With numeric passwords (like a PIN) each extra digit is ten times more difficult to "**brute force**" guess. 10, 10^2 (100), 10^3 (1,000), 10^4 (10,000)

Adding complexity (a combination of upper and lower case letters, punctuation) makes it even more difficult. 96, 96^2 (9,216), 96^3 (884,000), 96^4 (85,000,000)

Computers are fast and getting faster all the time, passwords that are too short or not complex enough can be "cracked" in fairly little time using brute force

More password issues

- Many people use weak or commonly utilized passwords
- Many people use “dictionary” words that are even easier to crack than brute force methods that try every possibility
  - “Pass-phrases” are an attempt to help these two issues
- Many people have multiple “accounts” and re-use the same password over and over. Compromise of one system means your discovered credentials might be utilized on many other systems
- Passwords are frequently put on a post-it note and stuck to computer screens or on the back of a device/phone
- Passwords may be intentionally shared with others (such as friends and family), or may be obtained by hackers via a variety of means

Password Best Practice Checklist

- Use long (16 characters or more), complex (letters, numbers, punctuation) passwords
- Use a different password on every system. If you can't handle that, at least use different credentials and passwords on each system that stores your most critical information (e.g. bank accounts) and use something else for "fun" sites
- Don't share your password with others
- Change your passwords periodically
- **Install a password manager** on each of your devices and learn to use it. This is a HUGE thing you can do to improve your overall security posture. There are several good products with "free" options such as LastPass,

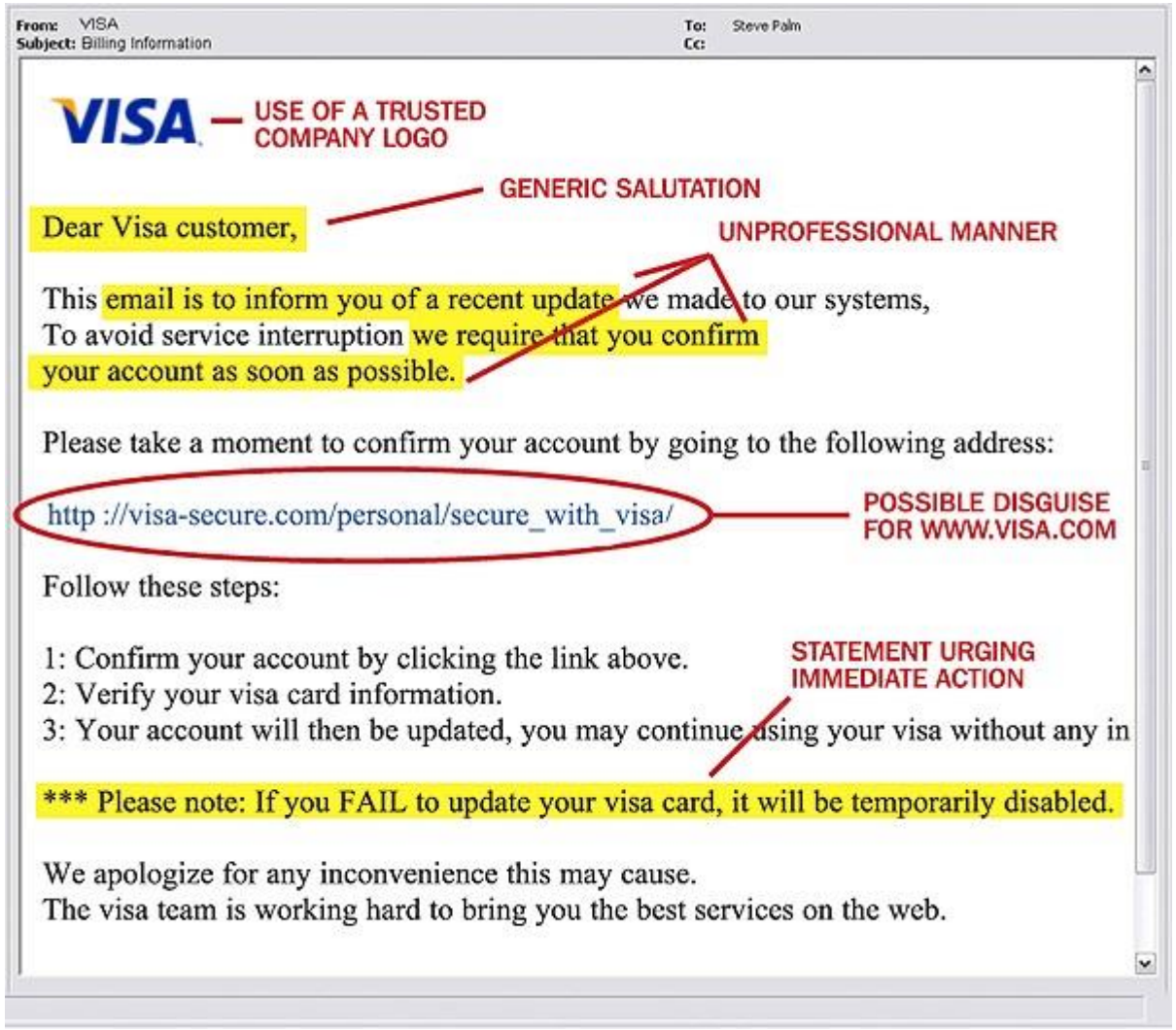
LastPass •••|

Even if you follow all best practices, there are many ways a “hacker” can obtain your credentials

- Brute force, dictionary attack, or cracking software
- You visit a non-secure website (no https), are using public wifi and they use a network packet sniffer.
  - using a VPN (Virtual Private Network) would mitigate this risk
  - UW provides the “Husky OnNet” VPN service to all students at no cost
  - Many commercial VPN services also available if you don’t want your traffic to be “on” the UW Network
  - Consider using UW “Eduroam” wifi when on campus instead of “University of Washington”
- Keyboard logger device on a public computer
- Compromise or “breach” of a site with your data and that data is not further encrypted
- They buy it on the “dark web” (we will discuss the “dark web” later)
- You tell them freely, you are tricked into telling them, or you log into a “fake” site that looks like the real thing via a “phishing” message

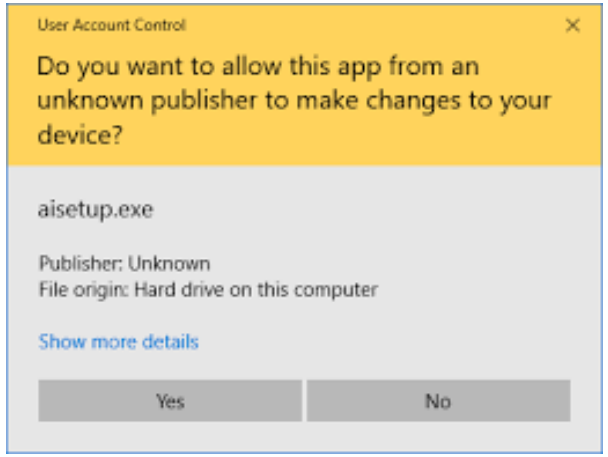
Phishing Messages – example of Social Engineering

- Attempt to deceive and trick us into clicking a link or taking other action
- In the past many were easy to detect
  - Lots of spelling errors and typos, very poor grammar
  - Links pointing to URL's in other countries
  - Suspicious email address, not quite right
  - An offer of $2 million from a long-lost relative
- Today many phishing messages are high quality, often no obvious way to tell
  - May mention your name directly
  - Have the logo of a company you do business with
  - Appear to be from a friend, an "official" organization like corporate IT or Microsoft telling you to do something for security reasons, to keep your email working etc.
  - Take you to a login page that looks just like the "real" login page you expect
- The University of Vermont IT organization recently sent a fake phishing email to all their faculty, students, and staff to see how susceptible users are, 85% clicked-it



Phishing Messages Best Practices

- By default assume any message asking you to click a link or provide any type of credential (userid, email address, password, financial info), or open an attachment is not real – it is phishing
- Assume that any message saying you have inherited a million dollars, or has other unexpected good news, is too good to be true
- If from an important person you know and uncertain, ask them
- If from an important company you do business with, call to verify. Alternatively initiate visiting the site yourself manually, not by not clicking the link, but by entering the URL yourself
- If you must click, hover-over the link and **inspect it carefully**
- Remember that phishing messages may also deliver “malware” to your device, they are not just looking for passwords. Don’t give permission for executable programs to run!



2FA, Two Factor Authentication
MFA, Multi-Factor Authentication

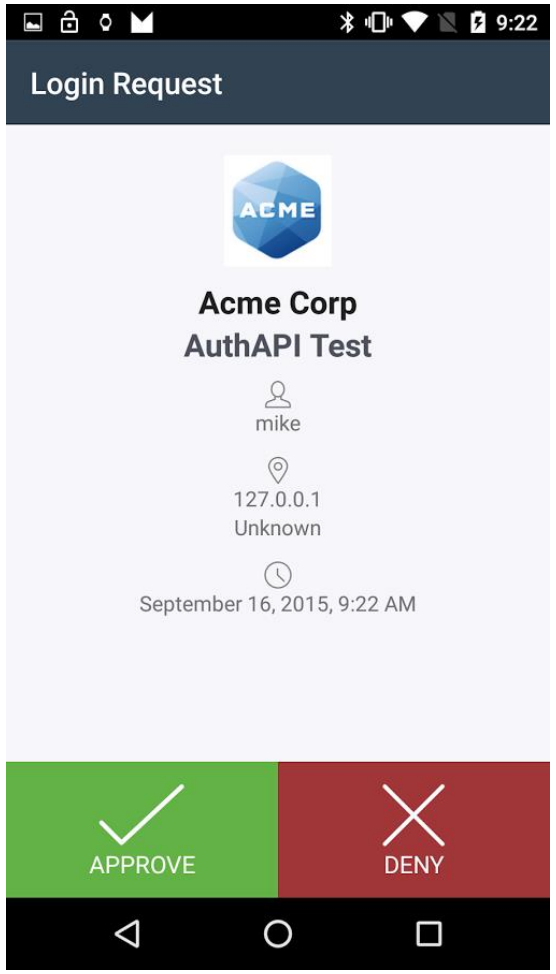
- 2FA and MFA allow us to add other factors besides “something I know” to authenticate

  2FA is a subset of MFA

- Most commonly with 2FA the “something I know” is my userid/password, the something I have is my mobile phone

- The second factor might also be a “YubiKey” or desk phone

- UW Workday authentication example



Advantages, Disadvantages

Can you think of some advantages of 2FA?

- More secure – need two factors to login
- You get notified of each login attempt and might detect an attack in advance
- Gmail, Microsoft, Facebook and many others now support 2FA

How about disadvantages?

- Not all systems support 2FA or enable it by default
- Requires you to have both factors at hand or no access - phone or Yubikey could be lost, you forgot it at home
- An extra step, takes extra time

- As a result many only use 2FA on sytems with their most critical information that needs protection – Payroll, credit card accounts, banks etc.

Authorization

The process of verifying that a person or agent is allowed to do what they are trying to do.

What do I mean by an “agent”?

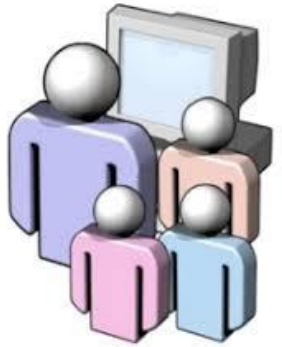
Expressed as a collection of permissions granted to a person or agent on a resource

Examples:

Can see your Facebook or WeChat posts
Can read the contents of a shared folder or file
Can make changes to a folder or file
Can edit a particular web page
Can see and change student grades in Canvas
Can request data from the UW student database

Note: authorization typically only applies to information at rest, not information in flight

Users



Most systems require “users” to authenticate first – so we can verify who they are.
We then can make authorization decisions that determine what they can do.

There are two primary “levels of privilege” a user might have

- Administrator, Admin, or “root” - the highest level of privilege, authorized to do anything
- Standard User – lower level of privilege, restrictions in place so you can only do what you are given permission to do

Typically administrators can do anything, including:

- Make system or configuration changes
- Install/remove/modify software applications
- Add or remove other users, create and manage groups (we will discuss groups in a bit), change passwords
- Grant rights and permissions to others, or change rights and permissions on resources

- When installing a new operating system “clean”, the person doing that install establishes who the administrator is and the initial admin password. They may add other administrators or “standard” users to the system at the same time.

Once initial setup is complete, best practice is to login as an Administrator **only when absolutely required**, this is called the principle of “least privilege”. Why would this be a best practice?

Administrator account concerns

- In companies a system administrator is often very knowledgeable, but they are people too and can make mistakes. If an administrator, admin, or root/super user makes a mistake it can be a disaster.

- If an administrator has their password compromised, if an administrator downloads a virus, if an administrator hits delete on a critical folder it can be a disaster.

- On many home PC's and Macs, people who are not very knowledge are often the "administrator" just because their account was the created first. If they do any of the above and it could also be a disaster.

- Why?
  Admins are authorized to do **everything** by default

- But…if that same person used a "standard" privilege account by default, and only became admin when necessary, the danger is substantially reduced.

- Because admin or root accounts are so powerful, they often are targets of cyber attack. Following best password practices for admin accounts (long and complex passwords) is critical

Groups

Groups are a collection of users that have something in common. Groups may be big or small and Admins create them whenever they want to control or limit access in a particular way.

Friends
Family
Parents
Kids
Kids under 15

Students at UW
iSchool Students
INFO 200 TAs
INFO 200 Instructors

Some example rights or permissions we might explicitly assign or revoke based on membership in a group

Can see my Facebook posts
Can view all the photos on our computer
Can see and modify the tax return folder
Can't see the tax return folder
Can't access wifi after 10pm

Can look at the UW student directory
Can download free Microsoft software
Can look at but not edit the upcoming quiz
Can look at and edit the upcoming quiz

A single user may be a member of many different groups

Permissions/rights

- Establish what you can or can’t do with a particular resource
- Assigned to users and/or groups, sometimes to other apps
- Using groups instead of assigning rights to individual users is preferred, much easier to manage over time

Operating system permissions for files and folders:

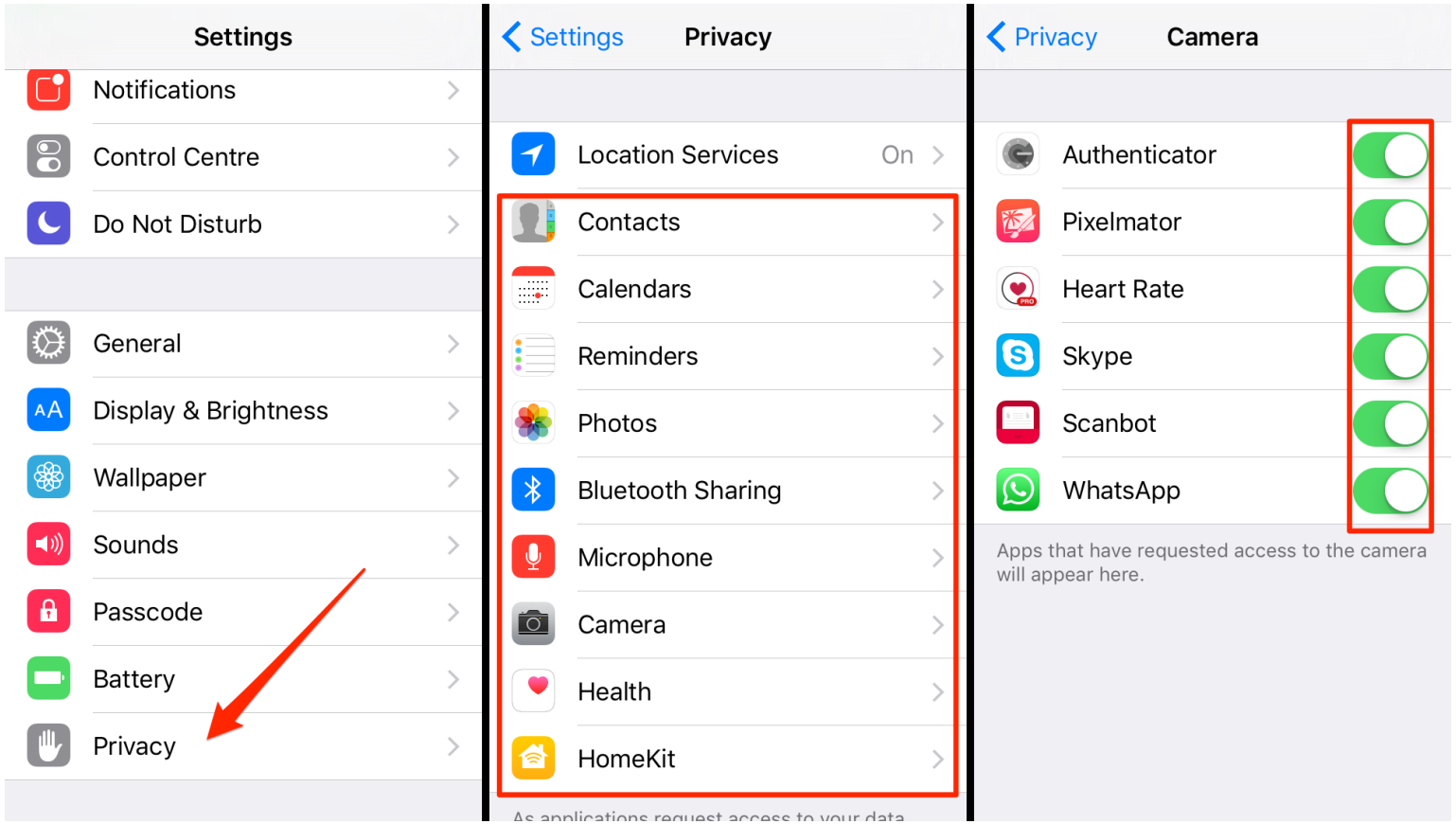
- Linux, macOS - read, write, execute (rwx)
- Windows – Full control, Read, Write, List Folder contents, more…

Applications may also assign rights to users, groups, or particular roles

e.g. Canvas – “Teachers” can see and update student grades

Some phone apps ask you to grant them permission to access to your photos folder, or allow them to see/modify your contacts, use your location

In addition to users and groups, phone apps may be assigned rights or permissions



How did these apps get these permissions?

Refresh:

What is the difference between

Authentication and Authorization?

Who you are

What can you do

Common Attacks Against Systems

Password attacks – dictionary, brute force especially against admin accounts

Social Engineering – Phishing

Exploits in operating systems or application software due to bugs

Malware

- AdWare – undesired popup ads or notifications appear
- Viruses – can delete files, steal information, install other malware – capable of replicating and spreading to other devices by running a program, clicking an attachment
- Worms – leverages system vulnerabilities, like a virus but doesn't require the user to do anything special
- Rootkits – remotely control a system
- Ransomware – holds your device captive, encrypts files – pay or lose them
- Spyware – collects information (login, credit cards, personal data) and reports back
- Trojan Horse – disguises itself as normal software but delivers other malware when installed
- Denial of Service or distributed denial of service – attempt to make a service function poorly, or not be responsive, could be from one computer or many computers located around the world
- BotNets – networks of computers that have been compromised and may be controlled from a central location, then instructed to do something malicious, such as initiate a denial of service attack

Who performs these attacks?

Black hats, gray hats, and white hats explained

Can be broken into added categories:

Script kiddies – don't know much, do it because it is "cool" or want to impress friends

Hacktivists – have a cause

Everyday criminals - a little skill but not much, may purchase tools on the "Dark Web"

Experts - extreme knowledge, they find vulnerabilities and create the attacks others use

Soldiers or Nation States – work for national governments to negatively impact another country or defend against attacks from others

Protecting yourself from Malware

- **THINK!**
- Only install software from known trusted sources
- Avoid downloading software, music, videos that you know are not free, for free
- Avoid dangerous sites like warez or adult sites
- Be very suspicious of installing any software that appears as a popup or says you need to scan your computer to fix a security or performance issue
- Be highly suspicious of links/URLs sent in email
- Be highly suspicious of email attachments
- Make sure you are logging in to your computer as a “standard” user and not a local admin
- Pay attention when your OS warns you about opening potentially dangerous files

- Use built-in anti-malware software, such as Windows Defender on Windows 10 or 3rd party alternatives, and keep it up-to-date

  Yes on a Mac too

  UW IT provides “Sophos” for free to faculty/staff/students

- Backup your device
- Keep your operating system and application software current

Backup

Protecting Information is also about being able to recover information if it is lost. Possible scenarios:

- Malware (viruses or ransomware) or other cyber attacks that delete or encrypt files
- Natural disaster
- System or coding failure
- User or system admin mistake
- Lost or stolen device

- Backups could be to local or on-prem devices such as external hard drives, backup tape, backup servers

- Alternatively or also, backup to the cloud

Delete, delete, delete…

- While backups are great, sometimes the best way to protect information is actually to delete it when you are done with it

  Why?

  - Some records, such as confidential email, text messages, files might be discoverable in a future legal proceeding
  - If you work for government some records may be considered public record (email) and you might not want all email conversations disclosed (remember there still are phones!)
  - You could be hacked, lose your laptop, etc.
  - So if the item is not subject to record retention requirements, and you no longer need it – deleting it may be the best way to protect that information

- Note: deleting a file or email doesn't necessarily mean it is permanently gone. Why not?

What else can you do?
Install System and Application Software Updates Promptly

Many system vulnerabilities are due to programming bugs in operating systems (Windows, macOS, and Linux), browsers (Chrome, Edge, Firefox), and applications software (Office, Photoshop, Acrobat, iTunes, etc.)

In general you want to:

- Keep your operating system as current as possible
- Keep your browser updated (most browsers auto-update by default)
- Keep you application software updated (every product)

Many users postpone updates for long periods, or assume they don’t need them

Many bugs are exploited by attackers or malware (Mac and Linux too), some are “zero day” exploits

Update Pace

- Microsoft Windows
  - Second Tuesday of each month is “Patch Tuesday”
  - Other security updates released depending on severity of risk
  - Twice a year, major updates and new features to Windows 10 are released
  - To check OS version, Settings, system, about or type “winver” in the lower left search box

- Apple macOS and iOS
  - Updates as necessary
  - Major new version of macOS and iOS typically annually (usually fall)
  - To check OS version on Mac, Apple Menu, About this Mac. On iOS, Settings, General, About.

- Google Android
  - Updates as necessary
  - Major new versions typically annually
  - To check version, Settings, About phone

- Note that all OS vendors eventually stop providing security updates for older OS versions

- Many mobile phones (Android) may never get major OS updates

- Wikipedia keeps track of what is the most current version of every OS.
  - macOS, Windows, iOS, Android

End Lecture