**Lecture 26: Best Practices for Social Media Security – Part 1**

**1. Creating Strong Passwords and Enabling Two-Factor Authentication**

**Creating Strong Passwords**: A strong password is crucial for protecting your social media accounts from unauthorized access. Weak passwords like "123456," "password," or your name can easily be guessed by hackers. Instead, follow these guidelines to create a stronger password:

* **Length**: Aim for at least 12-16 characters.
* **Complexity**: Use a mix of uppercase and lowercase letters, numbers, and special characters (e.g., @, #, $).
* **Avoid Personal Information**: Don’t use names, birthdates, or common words that might be easy for others to guess.
* **Use Password Managers**: Tools like **LastPass** or **1Password** can help generate and store complex passwords securely.

**Example**: A strong password could be something like **“E@!3LxP2f@Tr1”**—which is random, long, and difficult to guess.

**Two-Factor Authentication (2FA)**: 2FA adds an extra layer of protection. Even if someone gets your password, they can’t access your account without a second verification method.

* **How it Works**: After entering your password, the service sends a code to your phone or email that you must enter to complete the login.
* **Real-Life Example**: Facebook and Instagram offer 2FA. If someone tries to log into your account from a new device, you’ll receive a code to your phone, making it harder for hackers to break in.

**Why It’s Important**: Even if your password is compromised, the second factor (usually your phone) ensures that only you can access your account.



**2. Recognizing Phishing Attempts and Scams**

Phishing is when attackers impersonate legitimate businesses or individuals to steal your information. These attempts can come in many forms, like emails, social media messages, or fake websites.

**Types of Phishing**:

* **Email Phishing**: You might receive an email from a company, claiming your account has been compromised and asking you to click a link to “reset” your password. The link actually leads to a fake website that steals your details.
  + **Real-Life Example**: In 2016, the **Google Docs phishing attack** targeted millions of Gmail users by sending a fake email claiming to share a Google Doc. When users clicked the link, they unknowingly gave hackers access to their accounts.
* **Social Media Phishing**: Attackers may send you a direct message on Twitter or Instagram, claiming there’s a problem with your account and asking you to click on a link to resolve it.
  + **Real-Life Example**: In 2020, a hacker posed as a popular influencer on Instagram and sent out phishing messages to their followers asking them to enter login credentials for a fake "security check" site.

**How to Recognize Phishing**:

* Check for **unusual sender addresses** (e.g., from a slightly altered version of a real email address like **support@googgle.com** instead of **support@gmail.com**).
* Look for **typos** and strange language in messages.
* Always double-check the URL of links before clicking. Make sure it’s **https://** and the official website name.

**What to Do**:

* + **Don’t click on suspicious links**.
  + **Verify** with the official company directly via their website or customer service before providing any personal information.
  + **Use anti-phishing tools** that can automatically detect suspicious links in emails.

1. **Safeguarding Personal Information**



Social media platforms gather a lot of personal information, and it's essential to safeguard it from unauthorized access or misuse.

**How to Safeguard Personal Information**:

* **Limit What You Share**: Be mindful of the details you share online, including your full name, phone number, address, or birthdate.
  + **Real-Life Example**: **Facebook** had an incident where over **87 million people’s personal information** was harvested without consent by third-party apps, which were linked to the **Cambridge Analytica scandal**.

* **Avoid Public Sharing**: Don’t share personal details, like your exact location or travel plans, in public posts, as criminals may use this information for **identity theft** or **robbery**.
* **Profile Privacy Settings**:
  + On **Instagram**, you can set your profile to private, allowing only approved followers to see your posts.
  + On **Facebook**, you can adjust your privacy settings to control who sees your posts (e.g., friends, specific people, or only you).

