Great! I'm glad the first section is taking shape. Now, let's move on to the second half, which focuses on **online scams and computer security**. This segment can be a little more technical, but the goal is to make the information clear, actionable, and engaging for your senior audience.

Here’s a proposed outline and breakdown for the **second half of the class** (computer security-focused):

## **Segment Two: Online Scams & Computer Security**

### **Introduction to Online Security:**

1. **Importance of Online Safety**

* *Red Flag:* "It’s just a click away!"
* **Key Message:** The internet offers convenience, but also presents risks that seniors should be aware of.
* **Real-World Example:** Show how a simple click on a link in an email can lead to harmful consequences, like identity theft or a computer virus.

1. **The Growing Threat of Online Scams**

* *Red Flag:* "Phishing" or unexpected emails, pop-ups, or ads claiming urgency.
* **Key Message:** Online scams are becoming more sophisticated, targeting seniors specifically because of their trust and sometimes limited tech knowledge.
* **Real-World Example:** The evolution from "classic" scams like phishing emails to more advanced methods like social media scams.

### **Common Online Scams Targeting Seniors:**

1. **Phishing Emails & Texts**

* **Red Flag:** Email or text message from a bank, government agency, or familiar company asking for account info or login details.
* **Example:** Fake emails from “Amazon” or “PayPal” requesting your account info.
* **Prevention Tips:**
* Always check the sender’s email address carefully (spoofing is common).
* Don’t click on any links or open attachments from unrecognized senders.
* **Rule of Thumb:** If in doubt, contact the company or agency directly using their official contact info.

1. **Tech Support Scams**

* **Red Flag:** A pop-up or phone call from someone claiming to be from Microsoft, Apple, or another company, saying your computer is infected and offering to fix it for a fee.
* **Example:** A pop-up warning that says, "Your computer is infected! Call 1-800-XXX-XXXX for help."
* **Prevention Tips:**
* Real tech companies never cold-call or use pop-ups to alert you to security problems.
* Don’t share remote access to your computer with anyone unless you initiated the contact.
* **Rule of Thumb:** If you didn’t ask for help, don’t accept it.

1. **Online Dating & Romance Scams**

* **Red Flag:** Someone you meet online, who seems perfect, starts asking for money or gifts, especially after an emergency or crisis.
* **Example:** A "romantic partner" asks for money to cover a medical emergency or travel expenses.
* **Prevention Tips:**
* Be cautious when meeting people online, especially if they quickly become too personal or ask for money.
* **Rule of Thumb:** If someone you’ve never met in person asks for money, it’s a scam.

1. **Online Shopping Scams**

* **Red Flag:** Websites or sellers offering products at incredibly low prices.
* **Example:** A website selling electronics at a fraction of the price, only for you to never receive the item.
* **Prevention Tips:**
* Only buy from trusted, well-known websites.
* Check for reviews or look up the website for scam reports.
* **Rule of Thumb:** If it sounds too good to be true, it probably is.

1. **Fake Job Scams**

* **Red Flag:** A job opportunity that asks for payment for background checks or training materials.
* **Example:** A "work-from-home" offer that requires you to pay upfront for a course or materials.
* **Prevention Tips:**
* Legitimate employers never ask for money upfront for a job.
* Be cautious of vague job descriptions or offers that seem too easy to land.
* **Rule of Thumb:** If you’re asked to pay to work, walk away.

### **Basic Computer Security for Seniors:**

1. **Strong Passwords & Two-Factor Authentication**

* **Red Flag:** Using the same password for everything.
* **Key Message:** Simple or repeated passwords are a common way for hackers to gain access.
* **Tips:**
* Use different passwords for different accounts.
* Enable two-factor authentication wherever possible (e.g., Google, Facebook).
* **Rule of Thumb:** A good password should be long (at least 12 characters), and include a mix of upper and lowercase letters, numbers, and special symbols.

1. **Safe Web Browsing Practices**

* **Red Flag:** Clicking on unfamiliar links in emails, ads, or pop-ups.
* **Key Message:** Always make sure the website is secure (look for "https://" in the URL and a lock icon).
* **Prevention Tips:**
* Don’t download software or files from unknown sources.
* Don’t click on ads that pop up on websites or in emails unless you are sure of their source.
* **Rule of Thumb:** If you’re unsure whether a website is safe, don’t interact with it.

1. **Updating Software & Antivirus Protection**

* **Red Flag:** Avoiding software or system updates.
* **Key Message:** Keeping your system and apps up to date ensures they are protected against new threats.
* **Tips:**
* Regularly update your operating system, web browser, and antivirus software.
* Set automatic updates to make it easier.
* **Rule of Thumb:** Updates protect your computer from threats, so always install them when they appear.

1. **Recognizing and Avoiding Fake Websites**

* **Red Flag:** A website that looks strange, or offers things that seem "too good to be true."
* **Key Message:** Scammers create fake websites that mimic real ones to trick you into providing sensitive information or payment.
* **Prevention Tips:**
* Check the website's URL for typos or odd spelling.
* Look for security badges or a valid SSL certificate.
* **Rule of Thumb:** If a website looks suspicious, leave it and do further research.

### **Real-Time Demo: How to Spot a Scam**

If possible, provide a live demonstration showing:

* How to identify a phishing email.
* How to check if a website is secure.
* A quick overview of how to set up two-factor authentication on common sites.

### **Key Takeaways:**

* **Trust Your Instincts**: If something seems off, don’t engage.
* **Use Secure Websites and Passwords**: Only shop on secure sites (look for "https://") and use strong passwords with two-factor authentication.
* **Keep Software Updated**: Always install updates for your operating system, apps, and antivirus.
* **Ask Questions**: If you’re unsure about an offer, ask a trusted friend or family member before acting.

### **Q&A / Wrap-Up**

Encourage questions at the end of this session, where people can ask about specific online threats they may have heard about or encountered. It’s also a great time to remind them that it's better to take a few extra minutes to verify things than rush into something risky.

### **Handouts and Presentation:**

For handouts, you could create a simple checklist that seniors can follow for online safety, with spaces to jot down their questions or notes. These could include:

1. **Do’s and Don’ts of Online Safety**
2. **How to Spot Common Online Scams**
3. **Checklist for Setting Up Two-Factor Authentication**
4. **Password Best Practices**

Would you like help refining any part of this second section, or tips on making it more interactive for your senior audience? Let me know how you’d like to proceed!

**Prompt**: *I like how you've taken some of the format from session one and incorporated them here. You suggest some very good topics as well. I do want to kinda change gears a bit for the second half. I want to prevent the information from becoming stale and predictable. For example: For the second half I would like to focus on how personal information can be (or is) harvested and obtained by scammers, or even over-reaching advertisers. I would specifically like to discuss Microsoft, Google, and Apple as the three largest offenders of users privacy and personal information collection. Many online type scams require personal information to be even viable. For the second half, I think I would like to focus on these types of scams.*

Great direction! Shifting the focus to how personal information is harvested and used by scammers (and companies) will keep the class engaging and informative. You're right that understanding how personal data is collected—by both legitimate and malicious sources—will give your audience a broader view of the threats they face online. It will also give them a better understanding of how scams operate and how to protect themselves.

### **Segment Two (Revised): Online Scams, Privacy & Data Harvesting**

#### **1. Introduction to Personal Information Harvesting**

* **Red Flag:** “Just click ‘I accept’ to use this free app or service!”
* **Key Message:** Almost everything we do online involves some level of personal information collection. While some of this data is used for legitimate purposes (like targeted advertising or improving services), it is also a goldmine for scammers.
* **Real-World Example:** Demonstrate how just signing up for an online service or downloading an app can lead to personal data being harvested, sometimes without clear consent.

#### **2. How Scammers Obtain Personal Information**

* **Red Flag:** Giving away personal details without realizing it.
* **Key Message:** Scammers need data to make their scams more convincing. The more they know about a person, the more likely they are to succeed in deceiving them.
* **Scammers Use Data To:**
* *Create targeted phishing campaigns* (e.g., using details like recent purchases, travel plans, or personal interests).
* *Impersonate family members or friends* in scams like the “Grandparent Scam.”
* *Convince people to act quickly* by referencing personal details to make them believe the scam is legitimate.
* *Create fake identities* for social media or online marketplaces.

#### **3. The Role of Big Tech Companies in Data Harvesting**

* **Red Flag:** Signing up for a service and not fully understanding what you’re agreeing to.
* **Key Message:** Companies like Microsoft, Google, and Apple collect a massive amount of personal data, often under the guise of improving services or providing free products. However, this data can be used to track and manipulate users, and even fall into the hands of scammers or malicious third parties.

**Microsoft, Google, and Apple: How They Harvest Your Data**

* **Microsoft**
* **Data Collected:** Usage data, location, search history, email content (through Outlook), contacts, documents, etc.
* **How it’s used:** Microsoft uses this data to improve services, provide personalized ads, and improve their machine-learning algorithms.
* **Real-World Example:** When you use Microsoft Word or Excel, it might ask you to sign in with your Microsoft account. This allows Microsoft to track your usage, making it easier to target ads or provide “personalized” content.
* **Prevention Tips:** Opt out of personalized ads in Microsoft settings, limit location tracking, and review privacy settings regularly.
* **Google**
* **Data Collected:** Search history, location, browsing activity, YouTube history, emails (Gmail), calendar events, Google Maps, and even conversations (through Google Assistant).
* **How it’s used:** Google collects a large amount of data for advertising and personalization, and to train their AI. They target ads based on what you search for, what you watch, and even where you go.
* **Real-World Example:** If you search for a new refrigerator, expect to see ads for refrigerators or home appliance stores on various websites or social media sites shortly after.
* **Prevention Tips:** Regularly check your Google Activity settings to delete old searches, turn off location tracking, and manage personalized ads.
* **Apple**
* **Data Collected:** Location data, iMessages, Siri interactions, iCloud data (photos, files, contacts), app usage.
* **How it’s used:** Apple claims to anonymize much of the data, but it still collects a lot of information for improving its services and creating personalized experiences.
* **Real-World Example:** Apple can track your app usage through the App Store, sending you personalized app recommendations based on your history.
* **Prevention Tips:** Limit location tracking, disable personalized ads, and review the data collected through iCloud and Siri settings.

#### **4. How Scammers Leverage Data from Big Tech**

* **Red Flag:** Suddenly receiving a call or email about something you just Googled or mentioned in a message.
* **Key Message:** Scammers use publicly accessible information (or data they've obtained through breaches) to create targeted attacks that are more likely to trick you.
* **Scammers Access Data By:**
* *Collecting data from third-party breaches:* If a company you’ve used is hacked (e.g., Adobe, Facebook, LinkedIn), your personal information could be sold on the dark web.
* *Using publicly available data on social media:* Scammers can scrape social media profiles for details about your interests, family, and location to craft convincing scams.
* *Data brokers:* Companies buy and sell consumer data to build detailed profiles that can be sold to scammers.

**Real-World Example:** If your email is part of a breach, scammers can use it along with personal details they've scraped from Facebook or LinkedIn to send you phishing emails that look more legitimate.

#### **5. What You Can Do to Protect Your Privacy Online**

* **Red Flag:** Constantly clicking “Accept” without reading the privacy policy.
* **Key Message:** Being aware of what you’re sharing and taking steps to protect your data is essential.

**Actions to Protect Your Privacy:**

* **Review Privacy Settings:** Regularly check and update your privacy settings on Microsoft, Google, Apple, Facebook, and any other service you use. Turn off data sharing options wherever possible.
* **Limit Social Media Sharing:** Be cautious about sharing personal information (e.g., birthdays, family details, address, etc.) on social media.
* **Use Strong Passwords & Two-Factor Authentication:** Don’t make it easy for anyone to steal your information by using weak passwords or reusing the same password across multiple sites.
* **Be Aware of What You’re Clicking On:** Avoid clicking on links in unsolicited emails, texts, or ads that ask for personal information. Always verify before responding.
* **Use a VPN:** When browsing the web, using a VPN (Virtual Private Network) can help mask your location and prevent your browsing activity from being tracked.

#### **6. Real-World Demonstrations (Optional):**

* **How to Check What Data Google, Microsoft, or Apple is Collecting:** Walk through checking privacy settings on these platforms (e.g., showing how to access Google’s “My Activity” page, Microsoft’s privacy dashboard, and Apple’s privacy settings).
* **How to Opt-Out of Targeted Ads:** Show how to opt-out of personalized ads on Google, Microsoft, and Apple devices.
* **Social Media Privacy Settings:** Walk through Facebook or Instagram privacy settings to show how much personal data can be seen publicly.

#### **Key Takeaways:**

* **Think Before You Click:** Always be cautious about sharing personal information online.
* **Control What You Can:** Use privacy settings to limit how much data is collected by big tech companies.
* **Beware of Scammers Using Your Data:** Be vigilant, as scammers use information about you to craft convincing attacks.
* **Take Action to Protect Your Privacy:** Use strong passwords, two-factor authentication, and privacy-focused tools like VPNs to help secure your personal information.

#### **Q&A / Wrap-Up:**

Invite your audience to share their experiences and ask questions. Consider including examples or even demonstrations based on their input. This section will feel less formal and more interactive, with opportunities for real-time engagement.

### **Handouts & Presentation Ideas:**

For the handouts:

* **Personal Data Protection Checklist:** A step-by-step guide for seniors to follow for protecting their privacy online.
* **Big Tech Privacy Settings Guide:** A one-page handout with links and tips for adjusting privacy settings on Microsoft, Google, and Apple platforms.
* **Recognizing and Avoiding Data Harvesting:** A list of red flags and tips on how to avoid having their personal data harvested.

By adding this layer of understanding about how personal information is collected, it not only helps the seniors recognize common scams but also empowers them to take control of their privacy online.

Would you like any adjustments to this approach or additional details to flesh it out further?

**Prompt:** I have been considering comparing the vast amount of personal data that is collected electronically annually as compared with the number of letters (or glyphs) written (or typed) by human beings throughout history. Figuring the use of a single byte to represent a character (hand written or typed) as a conservative starting point, I calculated about 2 Petabytes of characters over the last 5,000 years.

That’s a fascinating approach! Comparing the vast amount of personal data collected with the volume of human-written characters can really emphasize the staggering scale of data collection today. It also helps to put into perspective how our current digital footprint is exponentially larger than anything seen throughout human history.

1. Your Calculation:

Let’s break it down and confirm the calculation.

Assumptions:

1 byte per character (for both handwritten or typed characters).

Number of characters per year: This could vary widely, but let’s start with an estimate.

Rough Estimate for Historical Data (over 5,000 years):

If we estimate a reasonable number of characters (letters, glyphs, etc.) written or typed annually across the globe, the total number would be a moving target. Let's start by considering:

100 billion characters per year globally (a very conservative number when you think of all the writing done across different mediums, from handwritten letters, manuscripts, printed books, to typed content).

5,000 years of human history with writing systems in use.

Calculation:

100 billion characters/year × 5,000 years = 500 trillion characters (500,000,000,000,000 characters).

Convert this to bytes: 500 trillion characters = 500 terabytes (TB) (since 1 byte = 1 character).

Scale this over time: If we compare to data volumes in terms of petabytes (PB), we get 0.5 petabytes (PB).

2. Comparison to Modern Data Collection:

Now, if we compare that to modern data collection:

Data collected annually by companies like Google, Facebook, and Microsoft, combined with personal data collection from all digital devices (smartphones, wearables, etc.), is in the hundreds of exabytes annually, which is a massive leap beyond the relatively small volume of historical character data.

Examples:

Google alone handles more than 40,000 searches per second (which translates to billions of queries per day). Each search can result in data being collected, analyzed, and stored.

Social Media platforms: Facebook, for example, stores and processes billions of user interactions (posts, likes, comments, photos, videos, etc.), each generating multiple data points.

The Contrast:

In the past, human beings wrote perhaps 500 terabytes of text over 5,000 years.

Today, the digital world generates data in exabytes annually. A single exabyte is 1 million terabytes!

3. Emphasizing the Exponential Growth:

By comparing the 500 TB of historical human text to today's vastly larger data volumes (reaching into the exabyte and zettabyte range), you really highlight how quickly data collection has accelerated.

This analogy could work in your class as a powerful visual to show just how much data is now being gathered on a massive scale, often without our direct consent or knowledge. It’s not just about what you type or write anymore; it’s about everything you do online, your location, purchases, browsing habits, and even your conversations.

Possible Class Tie-ins:

The “Surge in Data Collection” Trend: From handwritten texts to mass data collection by tech companies, and the role it plays in enabling both legitimate services and scams.

How personal data is collected: You could introduce concepts such as metadata (data about data), tracking cookies, location data, and digital footprints, explaining how even your smallest digital actions (e.g., browsing habits) contribute to this massive data pool.

Scams and Targeted Ads: You can use this analogy to explain how advertisers and scammers leverage this data to create personalized (and more convincing) scams.

Visuals for the Class:

You might even use a graphic to show the scale of data collected over time:

A timeline of personal data collection (from ancient written texts, to the rise of print, to the digital age) vs. data collection from digital companies today.

A scale comparison chart showing petabytes vs. exabytes, so students can visually understand the difference.

Let me know if you’d like more help refining the analogy or preparing visuals to accompany this discussion!