

# Presentation: Protect Your Online Accounts

Ages 13-18

**\*BEFORE PRESENTING:** Edit the first slide and be sure to log in to the Manager in order to show your branding.

---

## Slide 1 Sponsor Intro

### NOTES

Introduce yourself to the class and explain a little bit about your role. Go over your typical day, some of the things your financial institution offers (products or services relevant to the class), why you sponsor Banzai for their class, or why you think financially preparing for college is important. **Consider inviting the class to ask questions about you, your role, your financial institution, etc.**

### Sponsor Intro

Hi, my name is [YOUR NAME].

I work as [JOB TITLE] at [FINANCIAL INSTITUTION].

Banzai!

## Slide 2 Concept Overview

### NOTES

Introduce the topic briefly. **Ask the students if any of them have had trouble accessing one of their online accounts, whether they forgot their password, couldn't prove their identity, or their account was compromised.** It is frustrating to suddenly lose access to services that are integral to our daily lives, especially if we have invested money and time into it (pictures on social media, online game subscriptions, etc.). Luckily, there are simple guidelines to ensure our most important accounts are both easy to access and secure.



Internet Safety

## Slide 3 Presentation Overview

### NOTES

This slide serves as a table of contents that introduces the presentation. These are the specific topics you'll cover in the order you'll present them in.

### We're going to discuss...

- Setting Accounts
- Passwords
- Authentication
- Common Scams
- Personal Devices
- Staying Safe on Social Media

Banzai!

## Slide 4 Setting Up Accounts

### NOTES

The first step starts when they create an account. **Ask the students if they ever signed up for something they used once and then never used again.**

Be wary of sharing personal information including email addresses for trivial accounts. Not all sites are trustworthy and will sell email address or other personal information. A dummy email account is useful for sites they might only use once or are unsure of. This is an email they only check to verify account set up and they don't mind if it gets compromised or sent spam. If a site requires unnecessary personal information they can provide a clear fake response. For instance, First Name: Prefer, Last Name: Nottoanswer, but don't use other peoples real information. **Ask the students if they can think of any fun fake responses.**



### Setting Up Accounts

## Slide 5 Passwords

### NOTES

Passwords are often the only way to reliably access our digital accounts. **Ask the students if they know what makes a good password.**

**(1) Unique, Hard to Guess, and Easy to Remember** - Over the course of a lifetime they could make hundreds of password. The more password they have the harder it will be to meet these three requirements. It can be tempting to find one long awesome password to use for every site, but if one site gets compromised it will be easy for the hacker to access all their accounts.

**(2) Consider a Password Manager** - With a password manager they only need to remember one great password and the manager will take care of the rest. There are several options and they have been proven to be secure.

**(3) When in doubt, they can write their most important password down** - This ensures the password can't be accessed online, and they know where to find it if they forget. However, they still need to keep it safe and remember where they wrote it down in the first place.

**Your Financial Institution may have its own advice for password used to access their services that you can share.**

### Passwords

- Unique, Complex, and Easy to Remember
- Consider a Password Manager
- When in Doubt Write Them Down

Banzai!

## Slide 6 Authentication

### NOTES

Passwords are only one way to verify accounts. Extra steps might be needed, and while these can be cumbersome, they add a layer of safety. The downside is if the students are unable to verify themselves it can be difficult or impossible to regain access. Understanding how their important accounts will verify their identity can save a lot of future headaches

(continued on next page)

### Authentication

- Security Questions
- Two Factor Authentication
- Suspicious Activity

Banzai!

**(1) Security Questions** - Some sites will ask them to fill out the answer to a few security questions. These questions can have more than one reasonable answer, so they can record the question and response they give if there is any doubt.

For even more security, they can give a nonsense answer and save the answer in a secure location.

**(2) Two Factor Authentication** - Another common tool is using two factor authentication. This is when they sign in with a password and then receive a link or passcode sent to their phone or email to continue.

For even more security, there are authentication apps they can put on their phone and link to their account that provide an extra physical layer of security.

**(3) Suspicious Activity** - In most cases sites won't require authentication beyond a password, but if they log in from a computer that the site is unfamiliar with, or a strange location, they might need to provide more than what they are used to. The problem is that years can go by without needing to verify yourself, and in that time phone numbers change, apps are deleted and question answers are forgotten. Make sure they update their information for important accounts in case they need to verify themselves.

---

## Slide 7 Avoiding Common Scams

### NOTES

**(1) Urgent Messages** - They might receive a text or email with a link from one of their accounts regarding an issue that needs to be resolved. These messages are often scams. The pages they link to might look legitimate but could be a site designed to collect their login information. If anything looks suspicious (weird email address, strange url, misspelled words), avoid clicking on the link or, if you already have, exit the site without entering any information. If the message was legitimate, they can always log in through their normal method to check if anything is wrong.

No legitimate site is going to ask them to email or text their login information. **Let them know how your Financial Institution contacts their account holders.**

(continued on next page)

### Avoiding Common Scams

- Urgent Messages
- Too Good to be True Offers
- Sketchy Websites

Banzai!

**(2) Too Good to be True Offers** - If something seems too good to be true, it probably is. If someone is offering something for free, it means they are trying to get something, probably personal information or login info. Any actual sweepstakes or prize offering will have a number they can call and verify. If the offer doesn't have a number or they have a problem getting a hold of anyone, it's a scam.

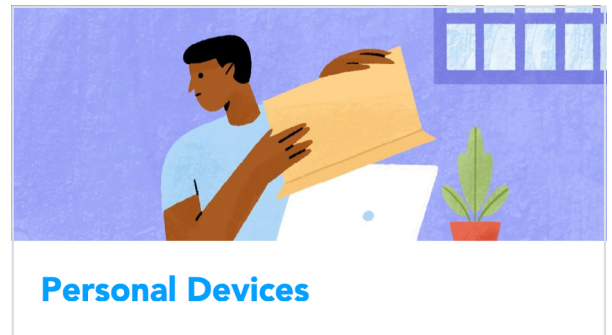
**(3) Sketchy Websites** - Web Sites that offer access to free media or games often contain misleading links and other tactics to collect personal information. Unlike too good to be true offers, they might deliver on their promise, but it's always a risk to get your media from illegitimate sources.

---

## Slide 8 Personal Devices

### NOTES

Personal phones, tablets, and laptops often automatically log into their accounts. It is important to have personal devices automatically lock after a period of inactivity, and If the students share a device, they should make sure their browser isn't saving login information. It's convenient to not have to enter a password everytime, but it also makes it convenient for anyone else who uses, finds, or steals the device to access information that doesn't belong to them.



## Slide 9 Interacting Online

### NOTES

Protecting your online accounts is more than just keeping your login and personal information safe. It also includes how you interact with others online.

**(1) Malicious Community Members** - Some services like online gaming and message boards, and social media allow users to communicate with each other. It's easier to trust advice or links given by community members, but at the end of the day they are still strangers and they don't know their intentions. Don't share personal information even if someone is trying to help, and double check any links they offer.

**(2) Unhealthy social media relationships** can be just as dangerous and strangers stealing their passwords. Students should be wary of anyone taking an abrupt and flattering interest in them, making uncomfortable requests or threats, or are in a sudden crisis that only the student can solve.

### Interacting With Others

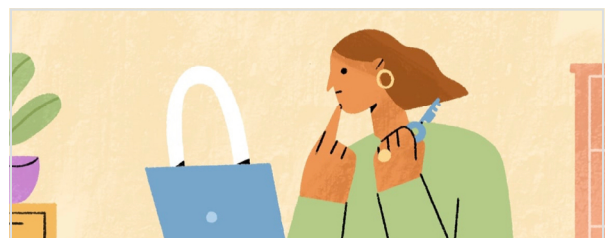
- Malicious Community Members
- Social Media Red Flags

Banzai!

## Slide 10 Presenting Yourself Online

### NOTES

The final thing to consider is protecting them from themselves. They may inadvertently be sharing information, comments, or media that they will regret in the future. More and more jobs, colleges, and organizations will take a look at how a candidate presents themselves online to make final decisions. What might seem like a joke now could cost them a future opportunity. A good rule of thumb is to behave online the same way they would behave at a party where everyone they know is there (friends, teachers, parents, grandparents, etc.), because ultimately their online presence can be accessed by everyone.



### Presenting Yourself Online

---

## Slide 11 Resources

### NOTES

Depending on class participation and discussion throughout the presentation, there may be extra time. These resources are helpful ways to go more in depth in protecting online accounts. First, students can take a more detailed look into security in a professional setting with the Workplace Cybersecurity Coach. One of the first tools is a password strength checker where the students can check if their password is secure. You could stop there or go through the entire coach having the students choose the responses.

Second, the Scam Checker Coach can help students check if a message they received is legitimate. You can provide an example to check or have the students provide real life examples.

---

### Resources

- Workplace Cybersecurity
- Scam Check

**Banzai!**

## Slide 12 Conclusion

### NOTES

Protecting our accounts is an important part of living in a largely digital society. Putting in a little work will help keep their information secure and easy to access, and being mindful while they interact with others will help represent them at their best.

### Make Sure Your Accounts are...

- Secure
- Easy to Access
- Reflect You at Your Best

**Banzai!**