Security
Episode 13

HOSTS: Alondo, Bevan, Jennifer
podcast@bebitwise.com

Recording Date: DD MMMM 2018

What Had Happened Was...?

[Team Advertises Millenial Night Featuring Avocados, Participation Ribbons, Napping Stations](#)

Do You Even Nerd/Geek?

Geek Battle Card

Say What?!!?!

Alondo

- There's a lot of facets for cybersecurity - protect your identity, your information, and your devices.
- Protecting your identity is incredibly important so that no one can impersonate you - Identity theft a high-growth and lucrative crime -
- Before the rise of technology, all you needed to confirm you were you was name, birthdate, and social security number
- Now - security questions, usernames, emails, etc.
  - Email address or cell phone number is synonymous with your name - people who know you know this public information
  - Usernames are like birthdates - small subset of people might know or be able to ascertain this information, but it's not something that can be used alone to imitate someone

- ○ Password or data that can be used to recover your passwords are like your SSN and should NEVER be divulged - even IT people have no need to have your password. If your identity is stolen, it can be incredibly hard to rectify, often taking years to fix - on top of that, most perpetrators are foreign and incredibly hard to track down.
- Protecting your information is the next important piece of being secure - In the real world, you'd be hesitant to tell people your work schedule and address for fear of someone knowing when you aren't home - Same thing on the internet - don't give enough information for someone to break into your sensitive data - Think about the questions used to recover your password
  - ○ family member's first, middle, or maiden names,
  - ○ schools you've attended
  - ○ old addresses or phone numbers
  - ○ make / model of first cars
  - ○ birthplace data
  - ○ Don't overshare on social media and don't divulge to anyone you don't personally know or trust. Watch what you post on those TBT
- The last thing is to protect your devices. Technology devices are like your entire ring of keys, you have to be careful with it. The most dangerous threat today is when a device has been compromised, and the owner doesn't even know.
  - ○ In the real world, a laundromat with weak security is the greatest threat if they are attached to a jewelry store or bank branch, even with high security.
  - ○ Computers with uninformed owners are compromised by software like botnets. These collective devices are used in tandem to to do things like attack big websites, or manually crack user passwords.
  - ○ Easy surprisingly easy to protect yourself - know that you have to invite malicious software in -
    - ■ Don't download anything that isn't from a trustworthy source - If it's free, there's a catch -

- Don't put sensitive information into a webpage unless you see the site is secure (should be a lock or the word SECURE in the address bar) -
- Never trust pirated apps or media -
- Never leave devices unlocked and unattended - use the device security recommended in our Money Ain't a Thang (Episode 7) -
- Always use two-factor authentication
  - Something you are
  - Something you know
  - Something you have

Bevan

[Six Cyber Threats to Really Worry About this year](#)

Jennifer

[Cryptography](#) / [Hashing](#)

Geek Out

No Geek Out Segment

Other References

Music

Intro and Outro music - Brasilia by Michael Glass

[See What Had Happened Was - Kutt Calhoun](#)

What Had Happened Outro Music

[Security - Otis Redding](#)

[Dixie Biscuits - Tape Five](#)