How Cyber Criminals Target High Schoolers

Why should a high school student be concerned about cyber security when they have barely done anything significant to make themselves a target?

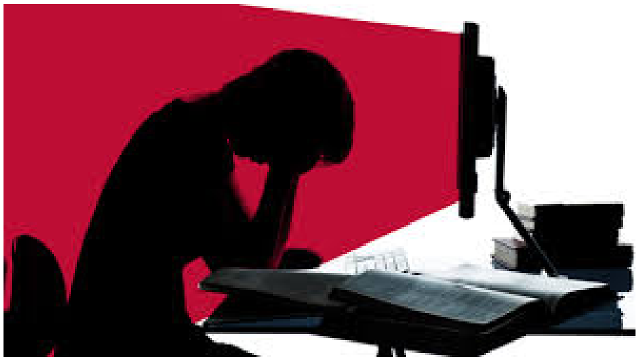
Simply because **that's how cybersecurity works.**

AKINS IT stated "Schools are the ideal target for hackers because they contain personal data seldom protected by similar cybersecurity policies used by other firms. According to reports, hackers breached a server with personal and financial info, such as admission information and student IDs. The attacks affect more than 200 million users."

The priority for cyber attacks is to gain information. The best line of defense is to increase the attacker's chances at failure.

A hacker can acquire and utilize student credentials for a wide variety of goals. Some of the most likely threats to high school students are:

1. Botnets
2. Ransom Attacks
3. Impersonation attacks
    a. Spoofing
    b. Formjacking
    c. Account Takeover (ATO)



1. **Botnets**

   Cyber criminals have utilized botnets for a variety of different reasons in the past. Nonetheless, the legitimacy of botnets, whether the user-generated information is real or fake, can vary based on the agenda the attacker is pushing.
   Student systems can fall prey to becoming part of a botnet.

   Cyber criminals can redirect users to external links, which infect their machines, making it part of a larger bot-network.

   This tends to happen when users access unsecure websites which prompt pop-ups in the background, or open new tabs.

Now, there are other explanations for pop-ups, such as forced advertisement. But some pop-ups can lead to sites that extract readily-available information from the user, including the user's email tags, IP addresses, and other critical pieces of data.

There is always a payment of some sort for 'free' online tools and software converting services. In some situations, a user's computer, attached with their user identity, can be conscripted to a botnet.

A user's machine can also be added to a botnet through malicious software that takes the form of an update for applications. For instance, an android user can receive a fraudulent update notification while browsing an insecure page:

> *"Have you got the latest Android update? Click here to begin installation."*

A loading procedure would promptly begin, not downloading the desired update, but uploading undesirably-personal information.

To the user, botnets can have repercussion such as;

- Having that user blocked from certain websites, or social media applications, due to that account being connected to malicious activity,
- The user becoming a suspect for illegal activity that they had no direct input in,
- Placing the user's family, friends, and other contacts at risk of fraud if the attacker were to use the user's account against them.

Botnets are successful due to their 'lowkey' nature of capturing information. One should always be mindful of website security to deter the risks of becoming another cog in an attacker's botnet.

2. Ransom Attacks and Ransomware

Ransom attacks are schemes that involve something of the user falling into the possession of an attacker, which the attacker uses as leverage to exploit that user.

As it relates to students, some attackers may use ransoms as a means to coerce students into using their parents' credit/debit cards to pay off the ransom.

Attackers know that students may not necessarily have the funds they require, so directing the attack towards the parents is the next best thing.

As a teen, nearly a decade ago, I was threatened by a ransom attack while traveling with my family. The threat began in the chat of a 3D mobile strategy game.

> *I was making friends with a player I met from the game's global chat feature. We made small talk about the game we were playing and chatted about ourselves a bit.*
>
> *Suddenly, the player brought up that they knew a way of getting freebies to my account, but I would have to provide my email address with its password info. I refused multiple times, but eventually caved in to the player's demands since I saw it as a friendly gesture.*
>
> *As you may have guessed, the player quickly demanded payments for my account after resetting my password and locking me out of it. It did not matter how much I begged, the player refused to return my account unless I paid for it.*
>
> *I was reluctant to pay the ransom, but was under a lot of pressure since the object being ransomed was my email account, filled with my college acceptances, and other school related documents, making it an excellent target for the attacker.*
>
> *I was able to use backup authentication software to regain my account, and I immediately redid my password login credentials.*

If I were more aware of my personal security on communication platforms, the situation could have been avoided entirely. Thankfully, the attacker was inexperienced and I was able to regain my account.

Conversely, ransomware attacks are done through the use of malware that prohibit a user from accessing their own digital accounts, files, media, online storage, and other forms of data.

These are ransom attacks too, but threat actors utilize software tools, and sometimes programming software, to lock users out of their systems.

These attacks are usually more centralized on businesses, and not so often on students; yet the likelihood of students being threatened by ransomware still exists, mostly depending on the social class, or status, of the student.

3. Impersonation Attacks

An impersonation attack is a general use term for different methods of deception, such as spoofing, formjacking, and account takeovers.

Impersonation attacks allow for a threat actor to gain access to something, somewhere, or someone, that would otherwise be inaccessible to them.

a. Spoofing

Spoofing is a type of impersonation attack that involves a threat actor pretending to be an entity they are not.

Spoofing is a key technique in successful deception.

Many cyber-criminals resort to spoof attacks to gain access to information on a subject that may not be directly related to the individual, or computerized system, they extract the data from.

~~For instance, Peach, the attacker, wants to find Coco's, the student's, and Coco's parents' Social Security Numbers (SSNs).~~

For instance, Peach—the attacker—wants to find Coco's—the student—and Coco's parents' Social Security Numbers.

Peach creates a new email address, posing as the Dean at Coco's school. Peach then designs and forwards an email to Coco, notifying Coco that their performance has improved over the past few months.

Peach assured Coco that their performance is deserving of a FAFSA for Coco's upcoming graduation. However, Peach would require the SSNs of Coco's parents in order to formally submit a FAFSA request.

Spoofing attacks are combined with social engineering methods to strengthen the attacker's likelihood of success.

The likelihood of success increases the more the individual's desires to reap the rewards of a false promise. The attacker, Peach, used the excitement of a scholarship award to fuel the chances of Coco meeting their demands.

The chances of Coco falling prey to this spoofing attack depends on Coco's digital security awareness, as well as their desperation for a scholarship.

b. Formjacking

Formjacking involves an outside entity receiving data through a user's direct connection to a website, or portal.

Attackers redirect traffic that the user inputs into the site, towards their storage location.

Students are especially at risk to formjacking due to the sensitive nature of information they are required to input in differing circumstances.

Students working towards scholarship opportunities are almost always required to fill out documentation requesting full names, date of birth, SSN, family information, and other invaluable details.

If not a scholarship, it can be an extracurricular activity, a part-time job or internship, volunteer work, online class-work, or whatever it is the student participates in needing access to information sharing over digital technology.

c. Account Takeover

An Account Takeover is what it sounds like. The attacker gains complete control of a user's account.

The likelihood of an account takeover attack on a school student is low, due to the complexity of the attack and the small value a successful attempt has on a student. However, the threat is still present.

There may be a greater likelihood for students from families of higher social class to be attacked, as this would be a way into their family's wealth.

There is also the potential for an attacker to sell breached student accounts online, or even to hold it as a ransom to the student it belonged to.

An account takeover can also occur as a white-collar crime, some form of revenge, or based on other rationales.

The possibilities here vary, but it ultimately depends on the motives of the attacker.

How To Respond

High school students should begin safeguarding their internet usage by practicing good habits of digital security.

Risk deterrence, or decreasing the likelihood of a threat's success, is a key technique to avoid becoming a suitable target to a digital threat.

Some good habits include, but are not limited to:

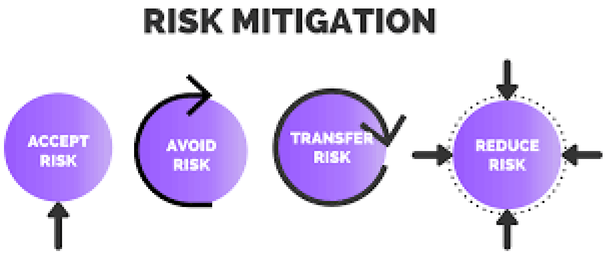
- Never share personal information with anyone,
- Never use insecure web pages,
- Continue learning different forms of offensive security to increase digital awareness,
- Always ensure the validity of unknown email addresses by checking with official sources first.
    - It's a good idea to check suspicious emails against those that are verified. If something appears to be off, contact the assumed sender to ensure they sent the email received. Sources such as '.gov' websites, and school office staff are a good start.

Nonetheless, the main idea here is prioritizing the security of information, especially since the goal of any cyber-threat is to obtain that information.

Risk mitigation also goes a long way, in providing assurance, that if an individual is 'hacked', the damages will not be as extensive.

Some good forms of risk mitigation include, but are not limited to:

- Using Two-Factor/Multi Factor authentication,
- Using reliable password recovery methods, such as 'name of high school mascot' etc.,
- Locking drives/folders on online databases, or within PC.



Overall, there is no definitive way of preventing a cyber-attack which is why risk deterrence, and sometimes risk mitigation, goes a long way in preventing, or reducing, the extortion of data.

References

CISM, Michael Swanagan, CISSP, CISA. “Types Of Security Controls Explained.” *PurpleSec* (blog), December 8, 2020. https://purplesec.us/security-controls/.

Feroot. “What Is Formjacking?” Accessed February 9, 2023. https://www.feroot.com/education-center/what-is-formjacking/.

“Formjacking.Pdf.” Accessed February 9, 2023. https://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/cyber-foundry/Formjacking.pdf.

GeeksforGeeks. “What Is an Impersonation Attack?,” August 5, 2022. https://www.geeksforgeeks.org/what-is-an-impersonation-attack/.

Heimdal Security Blog. “What Is a Botnet & How to Prevent Your PC From Being Enslaved,” July 22, 2021. https://heimdalsecurity.com/blog/all-about-botnets/.

Learning Center. “Account Takeover Attack (ATO) | Types, Detection & Protection | Imperva.” Accessed February 9, 2023. https://www.imperva.com/learn/application-security/account-takeover-ato/.

“Mercyhurst, Erie’s Public Schools Slate Cyber Training for High School Students | Mercyhurst University.” Accessed January 12, 2023. https://www.google.com/imgres.

Mimecast. “Impersonation Attack | Email Impersonation Attacks.” Mimecast. Accessed February 8, 2023. https://www.mimecast.com/content/impersonation-attack/.

Palo Alto Networks. “What Is a Botnet?” Accessed February 7, 2023. https://www.paloaltonetworks.com/cyberpedia/what-is-botnet.

Rakshit Devrupa. “Cybercrime Cases Against Women Spike Under Covid19 Lockdown.” *The Swaddle* (blog), May 4, 2020. https://theswaddle.com/cybercrime-cases-against-women-spike-under-covid19-lockdown/.

Today Software Magazine. “The Art of Phishing.” Accessed February 8, 2023. https://www.todaysoftmag.com/article/3181/the-art-of-phishing.

“The 5 Most Common Cyber Threats in Schools | Akins IT.” Accessed January 12, 2023. https://www.akinsit.com/the-5-most-common-cyber-threats-in-schools.

“What Is an Impersonation Attack? | UpGuard.” Accessed February 8, 2023. https://www.upguard.com/blog/impersonation-attack.

“What Is a Spoofing Attack? | Types & Examples.” Accessed February 8, 2023. https://study.com/academy/lesson/what-is-a-spoofing-attack-definition-types.html.