NAVIGATING NEW CHALLENGES THIS ACADEMIC SCHOOL YEAR

Published September 2020

INTRODUCTION

Students, faculty, parents, and guardians across New Jersey are preparing for the beginning of a new academic school year unlike any other. As academic institutions reopen for the 2020-2021 school year, the pandemic put a new spin on the typical back-to-school stress. Of the estimated 600 public school districts across NJ (not including charter or private schools), 434 will offer a hybrid option combining in-person and remote learning, 242 will open with an all-remote learning program, and 68 will offer all in-person classes, with many NJ colleges and universities also opting for all-remote learning. Consequently, for most academic institutions in the state, in-person classrooms and notebooks are substituted for video-teleconferencing (VTC) platforms and laptops for at least part of student instruction. The speed, in which these institutions and districts accommodated a remote learning environment, likely has or will result in many cybersecurity challenges. Additionally, the education sector continues to be one of the most targeted sectors by cyber threat actors. These factors, coupled with the unfamiliarity some may experience while navigating this new educational environment, increase the cyberattack surface and leave many users vulnerable to various forms of cyberattacks and other malicious activity.

As such, we have created this guide to adress cybersecurity concerns and compile best practices in an effort to assist students, faculty, parents, and guardians in addressing cyber safety and security concerns, navigating cyber-specific challenges they may encounter, and bolstering their cyber-resiliency. This compilation was created through coordinated efforts with the NJ State Police Cyber Crimes Unit (NJSP CCU) and the Digital Technology Investigations Unit (DTIU). The below sections will address best practices for device security, email and cloud service use, account security and the importance of multi-factor authentication (MFA), VTC security, internet safety, and securing home Wi-Fi routers and networks.

BACK-TO-SCHOOL DEVICE SECURITY

As the new school year starts, many devices with different operating systems and configurations will be exposed to numerous risks when connected to resources and networks not controlled by their academic institution. These devices are either personally-owned or provided by their academic institution and include desktops, laptops, tablets, mobile devices, and internet-of-things (IoT) products. These systems can provide threat actors with additional attack vectors to connect to networks, infect other devices, and exfiltrate data. Below are some general device cybersecurity best practices:

01

USE APPROVED RESOURCES AND PLATFORMS

Use only approved resources and platforms for academic communications to ensure they are trusted and secure.

02

KEEP HARDWARE AND SOFTWARE, INCLUDING MOBILE DEVICE OPERATING SYSTEMS AND APPLICATIONS, UP TO DATE

Keeping programs up to date ensures they are patched against known vulnerabilities that could be exploited by threat actors to gain unauthorized access to your device and/or data.

03

RUN AN UPDATED ANTI-VIRUS/ANTI-MALWARE PROGRAM

Keeping these programs up to date ensures they contain the latest signatures and data necessary to identify malicious software and processes.

04

CHECK PRIVACY AND SECURITY SETTINGS

Checking these settings will help manage your cyber risk and limit how and with whom you share information.

05

SET UP PARENTAL CONTROLS

Setting up parental controls allows the ability to control privacy and usage, content filtering, and location and monitoring settings to ensure internet use is safe and secure.

06

SECURE PHYSICAL DEVICES

Safeguard devices and ensure a password/passcode or biometric authentication is enabled for all devices to prevent unauthorized access in the event a device is lost or stolen, or USB or external device is inserted.

07

COVER AND/OR DISCONNECT YOUR CAMERA WHEN NOT IN USE

Covering or disconnecting your webcam and microphone when class is not in

session prevents malware from taking control of your camera to spy on you and your surroundings. Additionally, when the camera is in use, ensure no sensitive information is visible.

08 **BACKUP DEVICES**

Protect your schoolwork and information from malware, hardware failure, damage, loss, or theft by making multiple copies and storing them offline.

09 **IMPLEMENT PROTECTIVE TECHNOLOGIES.**

With remote learning, IT departments are advised to implement endpoint detection and response software, web content filtering software, host-based firewalls, device and file encryption, and keep devices updated with latest security patches.

BEST PRACTICES FOR EMAIL USE

Email is a commonly used method of communication in academic institutions and it is important to be vigilant about what is clicked on, downloaded, and transmitted, especially with the increase in social engineering tactics and spoofed domains. Threat actors may send phishing emails that appear to be from a trusted classmate, teacher, or colleague, and contain attachments or links that, if clicked. attempt to install malware or direct the target to a spoofed website to steal credentials or other sensitive information. Stolen credentials could then be used to send "trusted" emails to others in the academic institution to further compromise accounts or infect systems and networks with ransomware or other malware. Below are some general email best practices:

01 **IDENTIFY COMMON RED FLAGS**

Suspicious emails may contain external email tags but purport to come from internal sources, grammar and spelling errors, oddly placed upper and lower-case letters, incorrect or missing signature blocks or company logos, or words uncommonly used in everyday communications.

02 **WHEN IN DOUBT, THROW IT OUT**

If a message or a request looks suspicious or is "too good to be true," delete it.

03 **REFRAIN FROM TAKING ACTION, SUCH AS CLICKING LINKS OR OPENING ATTACHMENTS, ON ANY EMAILS RECEIVED FROM UNKNOWN SENDERS.**

If a message or a request looks suspicious or is "too good to be true," delete it.

04

CONFIRM THE LEGITIMACY OF EMAILS FROM KNOWN SENDERS THAT REQUEST SENSITIVE INFORMATION BY CONTACTING THE SENDER VIA A SEPARATE MEANS OF COMMUNICATION

Threat actors often impersonate legitimate and known individuals and academic institutions to convince targets to take a desired action that would compromise their device, data, or account.

05

SAY "NO" TO MACROS

If a file is accidentally downloaded, refrain from enabling macros or content as this is often a technique used to deliver malware.

06

VERIFY DOMAIN NAMES

Hover your mouse over the link to verify the URL before clicking or, instead, manually type the URL directly into the address bar of your browser. Once the website's legitimacy is confirmed, bookmark the page when needed.

THE IMPORTANCE OF SECURING ACCOUNTS

Account credentials—username and password—are the keys to the kingdom and the primary target of many threat actors. The sudden shift to cloud services, remote learning, and remote working has contributed to the increase in credential-based attacks. Cloud service accounts, such as Microsoft Office 365 and Google's G Suite, allow users to access email and documents, which contain mission-critical applications and sensitive data. If an account is compromised via credential theft or data breach, threat actors have the opportunity (absent MFA) to gain unauthorized access that allows them to further compromise accounts and systems, thus increasing the attack surface significantly. Examples include launching internal attacks, sending malware through email to students or teachers, stealing additional credentials, and accessing and stealing data from other applications in the cloud service. Although multi-factor authentication (MFA) may seem like an inconvenient step in addition to account credentials, it is an important one—not only to protect an individual account, but also the community at large. Below are some general account best practices:

01

REFRAIN FROM SHARING LOGIN CREDENTIALS OR OTHER SENSITIVE INFORMATION

Login credentials and other sensitive information should not be shared with

anyone or saved on your computer or cloud storage platforms. If requested, consult a parent or guardian first before sharing.

02 **KEEP ACCOUNT CREDENTIALS SAFE**

Keep a list that is stored in a safe, secure place offline and away from your computer, or use a service like a password manager to keep track of your passwords.

03 **USE UNIQUE, COMPLEX PASSWORDS FOR ALL ACCOUNTS**

Having unique passwords for each account prevents password reuse attacks, in which threat actors obtain your password for one account and use it to compromise an additional account using the same credentials.

04 **ENABLE MFA WHERE AVAILABLE**

MFA is the use of two or more factors in order to authenticate to an account or service. This significantly reduces the risk of account compromise via credential theft in which your password has been exposed.

05 **UPDATE PASSWORDS IMMEDIATELY FOLLOWING A DATA BREACH OR POTENTIAL COMPROMISE.**

Use a resource, such as haveibeenpwned.com, to determine if your information, such as an account password, has been revealed in a public data breach. Change exposed passwords for every account that uses it to protect against account compromise.

06 **USE THE NJCCIC INSTRUCTIONAL GUIDES TO IMPLEMENT SECURITY AND PRIVACY CONTROLS FOR ANDROID, FACEBOOK, GOOGLE, INSTAGRAM, AND TWITTER, AND CONFIGURE SIMILAR SETTINGS ON ALL OTHER ACCOUNTS.**

Tightening security and privacy settings will help to prevent account compromise and the unintended sharing of sensitive information and photos.

07 **REVIEW AND APPLY RECOMMENDATIONS FOUND IN THE NJCCIC POST HOW BIG IS YOUR FOOTPRINT?**

The smaller your digital footprint, the less publicly-accessible information is available for threat actors to more effectively target you.

08 **INVEST IN SECURITY AWARENESS TRAINING.**

Invest the time, money, and resources to ensure students, faculty, parents, guardians, and IT professionals understand risks, the latest cyber threats, and best practices. The NJCCIC is available by request to provide outreach

Presentations to inform users on current cyber threats and associated recommendations and best practices.

SECURELY USING VIDEO TELECONFERENCING PLATFORMS

Student and faculty engaged in remote learning environments will likely utilize a video-teleconferencing (VTC) platform for at least part of academic instruction. There have been several cybersecurity incidents involving VTC platforms since the start of the COVID-19 pandemic. VTC-hijacking – unauthorized individuals gaining access to a VTC meeting and displaying lewd, threatening, or otherwise inappropriate images or audio – has been one of the most prevalent threats facing those who use these platforms. Through security awareness and software updates, this threat is largely mitigated by applying the correct security and privacy settings on these platforms. Additionally, threat actors have impersonated various VTC platform via phishing emails claiming to contain a link to a virtual meeting. These links may result in the download of malware or being directed to phishing websites designed to steal user account credentials. Maintaining awareness of these various threats and tactics can greatly reduce victimization. Below are some general VTC cybersecurity best practices:

01 **REQUIRE A PASSCODE FOR ALL MEETINGS AND SECURELY SHARE THAT PASSCODE ONLY WITH YOUR INVITED GUESTS**

Once set, guests must enter the passcode in order to enter the meeting. This will prevent unauthorized individuals from joining a meeting.

02 **USE WAITING ROOMS AND REQUIRE APPROVAL FOR EXTERNAL PARTICIPANTS.**

Waiting rooms allow the meeting host to verify those attempting to gain access to the meeting. External participants are those with email addresses outside of the academic institution's email domain

03 **DO NOT SHARE YOUR MEETING IDS**

These IDs are unique to individual users and could be used to determine when a meeting is currently in progress.

04 **DO NOT REUSE MEETING IDS OR PASSCODES**

Using new IDs and passcodes for each meeting reduces the risk of an unauthorized individual obtaining information needed to gain access to a VTC

session.

05 **SEND LINKS TO MEETINGS DIRECTLY TO INDIVIDUALS AND DO NOT PUBLICLY POST MEETING LINKS**

Publicly posting meeting links could allow unauthorized individuals to access your meeting, particularly when other security settings are not in place.

06 **DISABLE PARTICIPANT SCREEN SHARING OR FILE SHARING AND DISABLE OR LIMIT AUDIO SHARING**

Disabling these features will prevent your meeting from being hijacked by others and allowing the sharing of inappropriate content.

07 **LOCK MEETINGS ONCE EVERYONE HAS JOINED**

Locking meetings prevents unauthorized users from gaining entry while the meeting is in session.

08 **AVOID POSTING PHOTOS OF YOUR MEETINGS**

Posted photos could provide threat actors with the associated meeting ID and information on meeting participants.

09 **DISABLE "ALLOW REMOVED PARTICIPANTS TO REJOIN" OPTION**

If an unauthorized participant is identified and removed, disabling this option will prevent them from regaining access to the meeting using the same account.

10 **DO NOT USE DIAL-IN NUMBERS FOR YOUR MEETINGS, WHERE POSSIBLE**

Anyone with the dial-in number and meeting PIN can join the meeting, and the individual's phone number identifier makes participant verification more difficult.

11 **KEEP ALL REMOTE LEARNING/VTC PLATFORMS UPDATED**

Enhanced security and privacy features may be implemented.

12 **ENABLE MULTI-FACTOR AUTHENTICATION (MFA) FOR ALL ACCOUNTS THAT OFFER IT**

MFA will prevent account compromise resulting from an individual gaining access to or guessing a user's password.

PLATFORM-SPECIFIC BEST PRACTICES & RECOMMENDATIONS

Google: Meet Security & Privacy for Education

Privacy & Security for Zoom Video Communications

Teachers: Top Features for Securing Your Virtual Classrooms & Enhancing Students' Learning Experiences (Zoom)

ENSURING INTERNET SAFETY

Technology can be a great educational tool, but may expose students to various risks if protective measures are not implemented. Children are often introduced to electronic devices at younger ages, and many are more technology-savvy than their parents or guardians. Children, teens, and adolescents excessively flocked to social media for a way to connect with friends and family during the pandemic. In our "always-on" society, children are one of the most vulnerable user groups as they are often exposed to heavy media saturation and potentially harmful material. Remote learning will only widen this exposure with the increase in screen time. Parents/guardians should check devices provided by their academic institution(s) to ensure content filters/blocks are enabled and contact the IT department or academic administration for further assistance, if necessary. Regular audits should be conducted by the IT department to ensure access is only permitted to appropriate online educational materials, as well as to confirm that updates have been applied. Additionally, NJ academic institutions should provide both students and parents/guardians with the Responsible Use Policies (RUPs), also known as Acceptable Use Policies (AUPs), which outline the terms of use for school-issued devices and consequences for violations of these policies. Below are some risks associated with increased internet exposure that may impact children, and the resources parents, guardians, and teachers may use to assist them through these issues.

01

OVERSHARING PII ONLINE

Sharing of personally identifying information (PII) can provide threat actors information necessary to engage in cyber-criminal behavior, identity theft schemes, or, in the case of children, online predation. Students are encouraged to be selective with the information they share on social media platforms, remote learning environments, and during video teleconferencing sessions. PII includes the following:

- Full Name
- Age
- Physical and Email Addresses
- Phone Number
- Social Security Number
- Full Birthdate

02

ENGAGING IN OR BEING A VICTIM OF CYBERBULLYING

Cyberbullying is a form of bullying that takes place over digital devices, such as

smartphones, computers, and tablets. Cyberbullying can be conducted via text, on social media apps, instant messages, and in online gaming arenas. It includes sending, posting, or sharing negative, harmful, false, derogatory, or personal content about someone without their consent, causing embarrassment or humiliation. Many children attempt to conceal their experiences; therefore, it is important for teachers, parents, and guardians to be aware of warning signs that a child may be experiencing cyberbullying. It is important to have conversations with children and stay engaged. Some instances cross the line into unlawful or criminal behavior. For more information visit stopbullying.gov.

03

VIEWING OR POSTING INAPPROPRIATE CONTENT

Children can unintentionally encounter inappropriate material, such as sexually explicit content, or otherwise disturbing images or videos. Ensure content filters and security blocks are in-place to protect children from exposure. Likewise, posting inappropriate content is also a concern. It is important to review with children the types of inappropriate content, including:

- Hate Speech
- Pranks
- Offensive Language
- Threats of Violence
- Underage Drinking or Drug Use
- Explicit Photographs of Themselves or Others

There can be immediate and long-term consequences for posting inappropriate content online affecting children for years to come including:

- Damage to their reputations
- Punishment if a post breaks the academic institution's rules or policies
- Charged with a crime if they are breaking a law
- Hinder acceptance to college, receiving a scholarship, or getting a job in the future

04

SEXTORTION

Children may become victim of sextortion, or threatened to distribute private and sensitive material if not compliant with requests of sexual images, favors, or money. Sextortion schemes may also utilize ransomware, whereby the individual's files are encrypted and the threat actor demands payment for the victim to regain access to their files.

05

BEWARE OF ONLINE PREDATORS

The National Center for Missing and Exploited Children (NCMEC) received almost double the number of online enticement reports and CyberTipline reports in the first half of 2020 compared to the same timeframe in 2019. The FBI also published a news release stating that school closings due to COVID-19 presented potential for increased risk of child exploitation. Online predators groom victims by building their trust, feigning common interests, or sympathizing with them, and eventually attempt to set up an in-person meeting to move forward with manipulation and seduction. Predators frequent the places children access such as social networks, chat rooms, blogs, message forums, etc. Some grooming techniques may be displayed as:

- Learn about the child's interests - movies, music, hobbies
- Become their "friend" - listen and sympathize with their problems/issues
- Send gifts to get attention and affection
- Gradually build to sexual content through conversations, photos, and videos
- Evaluate which child to attempt to meet in person

Adults who discover any of the above indicators should contact local law enforcement, the NJ State Police Digital Technology Investigations Unit (DTIU), or FBI.

ADDITIONAL INTERNET SAFETY RESOURCES TO ASSIST STUDENTS, PARENTS, GUARDIANS, AND FACULTY

NCMEC Online Safety Resources for Virtual Back to School

NJ Department of Education – Safe and Ethical Use of Computers

NetSmartzKids

NSTeens - Educators

Internet Safety Brochure for Parents

Stop Think Connect

Internet Crimes Against Children Task Force

GetSafeOnline.org

FBI

NJSP Cyber Crimes Unit

NJSP Digital Technology Investigations Unit

SECURE YOUR HOME WI-FI

To accommodate remote learning, students will use various devices that require an internet connection for their academic instruction. These devices will likely use a home wireless (Wi-Fi) network; however, the Wi-Fi router may not be set up securely. If a Wi-Fi network is left unsecured, a threat actor could potentially gain unauthorized access to the network and the devices connected to it. As a result, personal, financial, and otherwise sensitive data could be exposed, and their access may lead to other types of malicious activity. Below are some recommendations to help protect your network, data, and devices from unauthorized access and other malicious activity; additional details for implementing the recommendations, as well as steps to set up a Wi-Fi router, can be found in the NJCCIC Configuring & Securing a Home Wi-Fi Router Cybersecurity Guide.

01

CHANGE THE ROUTER DEFAULT USERNAME AND PASSWORD

Default router credentials are often publicly available and can be used to gain unauthorized access to your network.

02

CHANGE THE NETWORK NAME (SSID)

Default SSIDs may give away the router's model, which could provide threat actors information necessary to obtain the router password (if using default credentials) or determine potential vulnerabilities that could be exploited.

03

ENABLE WPA2 WITH AES (OR WPA3, IF AVAILABLE)

Wi-Fi Protected Access versions 2 and 3 (WPA2/WPA3) are both recommended options for ensuring data on devices connected to the network is properly encrypted and secured.

04

UPDATE YOUR ROUTER'S FIRMWARE

Unlike software that provides automatic updates or prompts users to install updates, Wi-Fi router firmware needs to be manually downloaded and installed. Without firmware updates, routers may contain known vulnerabilities or use outdated encryption that could compromise the security of the network.

05

CREATE SEPARATE NETWORKS FOR DEVICES

Creating separate Wi-Fi networks for groups of devices with similar purposes and/or sensitivity can help to prevent an entire network of devices from being compromised if a threat actor is able to gain unauthorized access to one device or network. For example, keep internet-of-things devices on one network and mobile devices on another.

06

PLACE THE ROUTER IN THE CENTER OF YOUR HOME

This placement provides the best coverage for the devices in your home, while also making it less likely that the signal will be strong enough for someone outside your home to connect to your network.

THE ABC'S OF THE NJCCIC CYBERSECURITY BEST PRACTICES

Account and device security
Backup data and keep multiple copies offline and offsite
Cyber hygiene
Data protection
Email security
Firewall protection
Gather threat intelligence
Hardening systems
Incident response
Join NJCCIC membership and other security mailing lists
Knowledge and information sharing
Lock screens and devices
Multi-factor authentication
Network security
Online presence and safety
Patches and updates
Question and report suspicious activity
Risk management
Simulation exercises and training
Third-party vendor management
Use strong, unique passwords
Virus and malware protection
Wireless security
X out of suspicious communications
Yield and think before clicking
Zero-tolerance for acceptable use

For more information, please visit our website at cyber.nj.gov.