SECURITY IS EVERYONE'S RESPONSIBILITY

CYBERSECURITY AWARENESS MONTH

OCTOBER 2020
WWW.NISDTX.ORG

Cybersecurity is more important now than it has ever been.

By Cara Carter
Executive Director of Technology

As our world becomes more digital, school systems become more vulnerable to cyberattacks. It is crucial that both staff and students know the importance of their impact on cybersecurity. We aren't only educating the global citizens of tomorrow. We are helping mold their digital footprint and identity, and are responsible for safeguarding their personal information and our own data systems.

With such high stakes, a school district has a lot to lose if we don't make this a top priority.

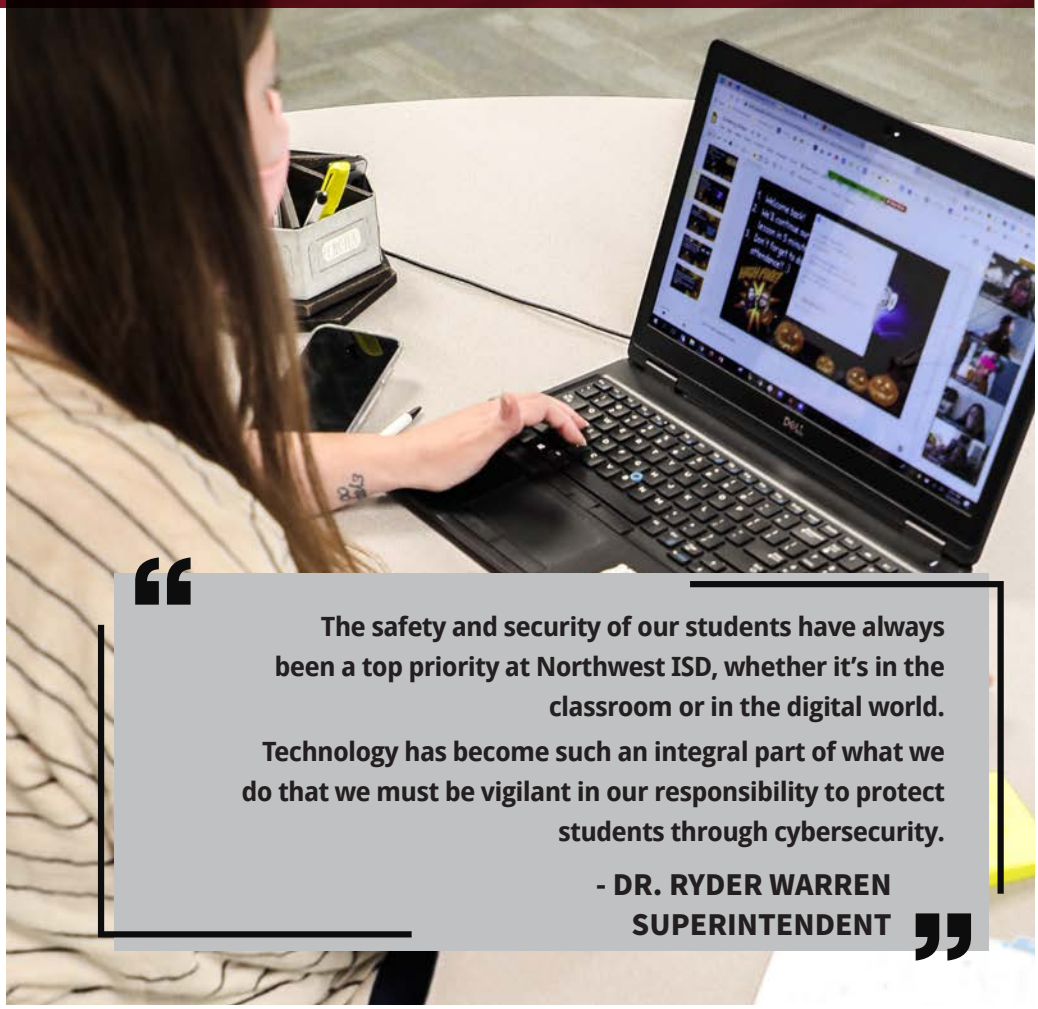
Threats are increasing at an alarming rate, and even with high-level engineers and sophisticated backend systems, we are all still vulnerable to potential threats.

It's you — the person behind the keyboard, the teacher helping a student log in to their Chromebook for the first time, the assistant principal emailing a student's parents — who are our first line of defense. You play a bigger role than you could ever imagine in keeping yourself, others, and the entire district safe.

During Cybersecurity Awareness Month, let's make a commitment to recognize our personal responsibility and the role we play in this digital landscape.

DON'T FALL FOR PHISHING!

They're looking for access and information:



> **The safety and security of our students have always been a top priority at Northwest ISD, whether it's in the classroom or in the digital world.**
>
> **Technology has become such an integral part of what we do that we must be vigilant in our responsibility to protect students through cybersecurity.**
>
> **- DR. RYDER WARREN**
> **SUPERINTENDENT**

HACKERS POSE AS PARENTS TO TARGET TEACHERS & SCHOOLS

Think twice before opening that email attachment — it might not actually be a student's homework assignment.

In a new targeted cyberattack, hackers are posing as a parent or guardian submitting an online assignment on behalf of a student, according to TechRadar. They claim the student encountered technical issues when trying to submit the assignment themselves.

But instead of attaching an assignment to the email, attackers are sending teachers a document to infect their computer with ransomware.

The attackers can then demand a ransom for control of the school district's systems.

At least six Texas school districts have experienced ransomware attacks so far this year, according to the Houston Chronicle.

Sheldon ISD, located in northeast Houston, paid more than $200,000 to hackers in March to regain control of its network.

And the number of cases continues to rise. With only three months left in the year, 289 cyber incidents have been reported publicly by US schools, according to the Wall Street Journal.

PASSWORD PROTECTED

Don't use the same password for multiple accounts.

Setting a strong password is one of the best ways to protect your information online.

Use a phrase or sentence to create a strong password. This could be something like a line from your favorite song, or a quote that you admire. String together the first letters of each word in the phrase for a hard-to-crack string of random letters.

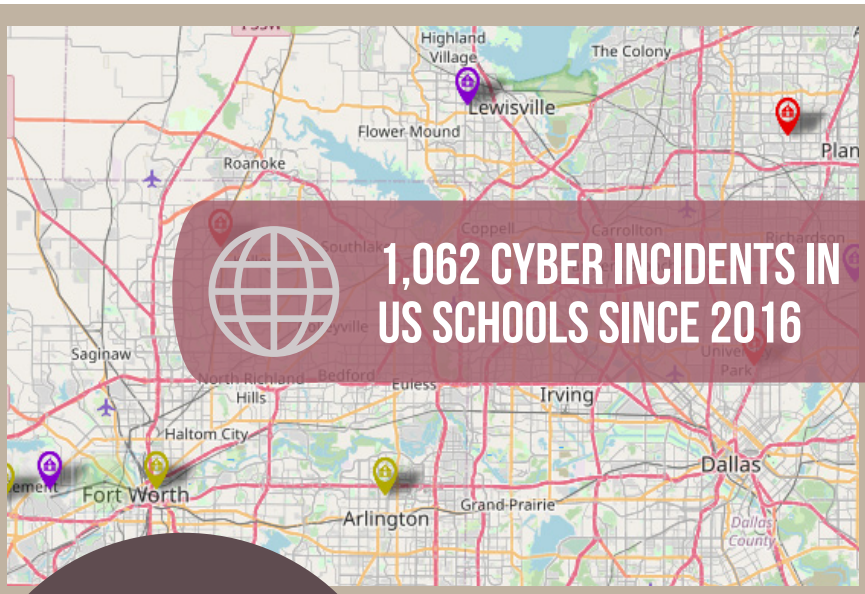
Combine numbers, special characters, uppercase and lowercase letters. Avoid replacing letters with look-alike symbols.

Don't use the names of people, pets or words found in the dictionary. Cybercriminals use programs to easily run through lists of these words.

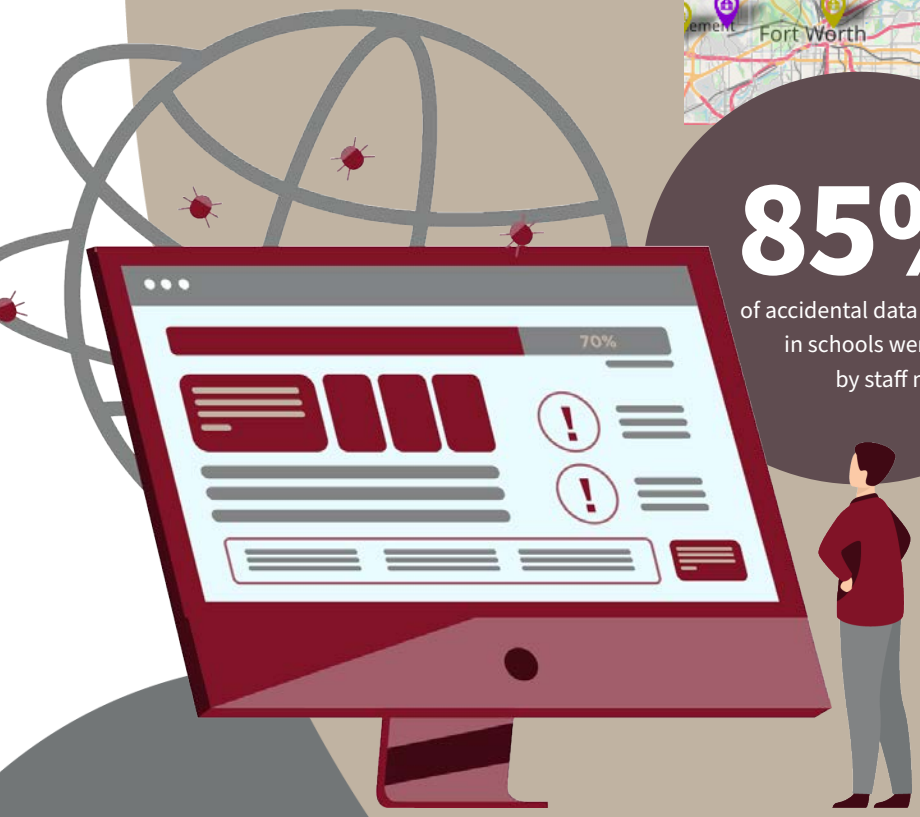
Use password management software to store and encrypt your passwords, and log in to websites. This will allow you to remember one master password and still keep your information secure.

IT CAN HAPPEN ANYWHERE

Student data breaches occurred more often in larger, wealthier, suburban school districts, according to a report by the US Government Accountability Office.



1,062 CYBER INCIDENTS IN US SCHOOLS SINCE 2016



85%

of accidental data breaches in schools were caused by staff members.

A LOOK AT NORTHWEST ISD:

13,420

ATTACKS PREVENTED THIS MONTH FROM 621 UNIQUE SOURCES

FAMILY HUB EMPOWERS PARENTS TO TALK TECH

Northwest ISD has been teaching digital citizenship to its students for the last decade. But as students become more immersed in technology every day, those lessons are even more important after the dismissal bell rings.

The Digital Citizenship Family Hub gives parents the tools to continue conversations about how to interact online and be a good global citizen.

Content is tied directly to NISD's digital citizenship curriculum, and highlights social-emotional targets that students are working on in other areas of their education.

"The world is changing and technology is changing," said Kylie Lloyd, instructional technologist. "We have to make sure our students have the resources they need to succeed in that environment."

Just as teachers help guide parents through teaching the "new way" of doing math, they've got to help parents understand the challenges kids face in today's digital world.

"We aren't only trying to educate kids to navigate through an ever-changing and even more complex digital realm," said Jason Sanders, director of instructional technology. "We've also got to empower parents to have those conversations and feel confident in what they're talking about."

> **"TECHNOLOGY is not meant to be an isolator. It's supposed to CONNECT us.**
>
> **By empowering students with skills and strategies to connect safely and productively, we are preparing them to successfully navigate their future."**
>
> **- JILLIAN PHILLIPS**
> **COORDINATOR OF INSTRUCTIONAL TECHNOLOGY**

Principal Lisa Ransleben shared the Family Hub with Justin Elementary parents after some students created fake social media accounts to impersonate classmates. She said it was invaluable to have that resource ready to go.

"The Family Hub empowers parents to be able to have conversations about the choices students make online," she said.

ADDITIONAL RESOURCES

Northwest ISD Digital Citizenship Family Hub
Northwest ISD HelpDesk
Common Sense Media
K-12 Cybersecurity Resource Center

SIMPLE STEPS TO CYBERSECURITY

We're all in this together — do your part to protect our systems.

SET UP PASSWORD RECOVERY.

This will secure your Northwest ISD account and ensure access when district offices are closed.

Log in to the NISD Portal, choose Settings, and click on the Recovery tab to display the password recovery options. You can also change your password anytime.

If password recovery isn't set up, you'll need to contact the HelpDesk if you forget your password.

Setting up password recovery outside of the Technology HelpDesk (817-698-1000) is the only way to ensure 24/7 access to your account.

REPORT PHISHING EMAILS.

Phishing scams actively aim to steal login credentials or other sensitive data.

These emails should be reported in Outlook, so the technology department can track the email and see if the NISD system has been compromised. Here's how to report them.

Spam emails are unsolicited messages sent to bulk lists trying to sell goods and services.

While annoying, these emails are usually commercial in nature and not expressly malicious. They aren't trying to gain access to your account.

UPDATE DEVICES REGULARLY.

Windows frequently provides software updates to protect against security breaches.

If your laptop is not consistently updated, NISD will have to force critical updates to your computer. Forced updates can happen at the most inconvenient times. Update regularly to control when software updates occur. Check to see if your device has updates available.

SHARE STUDENT DATA SECURELY.

By law, student data must be shared securely.

If you are sending student data in an email message, that data might not be protected. Instead, share the information via a Google Drive link to make sure it is protected against security threats. Customize permissions according to time frame and level of access needed.