CYBERSECURITY & INTERNET SAFETY

A practical guide for new Fort Bend ISD employees

Protect students. Protect coworkers. Protect the district.

Every employee helps safeguard district accounts, devices, data, and learning environments. Use this guide during onboarding and keep it as a quick reference.

THE THREE-SECOND PAUSE	Before you click, sign in, share information, or approve an MFA request, stop and ask: Was I expecting this? Do I recognize the sender and destination? Does the request make sense?

Your first-day security checklist

- Set up the district-approved multi-factor authentication (MFA) method.
- Register your account recovery methods at my.fortbendisd.gov.
- Create a unique, strong password or passphrase and never share it.
- Know how to contact the IT Help Desk: 281-634-1300.
- Use only district-approved devices, applications, cloud storage, and data-sharing methods.

IF SOMETHING FEELS WRONG	Stop. Do not click again, reply, approve, or forward the message. Contact the IT Help Desk and follow district reporting procedures.

1. Recognize and stop phishing

Phishing is a social-engineering attempt to trick you into revealing information, sending money, opening a harmful file, or signing in to a fake website. It may arrive by email, text message, phone call, QR code, social media, or collaboration tool.

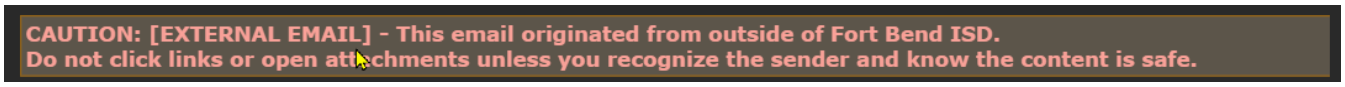
Common warning signs

- Unexpected urgency, threats, secrecy, or pressure to act immediately.
- A sender name that looks familiar but the actual address is unusual.
- A link whose destination does not match the displayed text or expected site.
- Requests for passwords, verification codes, gift cards, payroll changes, student data, or confidential records.
- Unexpected attachments, invoices, shared documents, QR codes, or login prompts.
- Spelling, branding, tone, or context that does not fit the sender.

What to do

DO	DO NOT
Verify unusual requests through a known phone number or a new message.	Do not use contact information supplied in the suspicious message.
Hover over links when possible and inspect the destination.	Do not click links or scan QR codes simply to “see what happens.”
Report the message using the district-approved process or contact IT.	Do not reply, forward widely, or continue interacting with the sender.
If you entered credentials, contact IT immediately.	Do not wait for signs of account misuse.
EXTERNAL EMAILS	Treat unexpected external messages with extra care. A familiar display name does not prove who sent the message.

External E-Mails are tagged with the message below so that you can quickly and easily identify a message from outside Fort Bend ISD.



2. Use strong, unique passwords

- Use a long passphrase that is memorable to you but difficult for others to guess.
- Use a different password for every account. Never reuse your district password on personal sites.
- Avoid names, birthdays, school mascots, addresses, keyboard patterns, or predictable substitutions.
- Never increment an old password by changing only the final number or character.
- Never share a password or one-time verification code with anyone, including someone claiming to be IT.

- Use an approved password manager if the district makes one available for your role.

3. Multi-factor authentication (MFA)

MFA adds another identity check beyond your password. It can reduce the chance that a stolen password alone will allow someone into your account.

Approve only sign-ins you started

- Read every prompt. Confirm the application, location, and number shown.
- Never approve an unexpected request, even if repeated many times.
- Never give a verification code to another person.
- If you receive an unexpected MFA prompt, deny it and contact the IT Help Desk.
- If you are unsure, stop the sign-in and begin again from a trusted district bookmark or portal.

MFA FATIGUE ATTACK	Repeated prompts may be an attempt to wear you down. Deny unexpected prompts. Do not approve one just to make the notifications stop.

4. Protect district data

District information may include student records, employee information, operational data, credentials, and other sensitive content. Access and share only what is needed for your assigned work.

- Use district-approved storage, sharing, and collaboration tools.
- Confirm recipients before sending email, sharing links, or granting access.
- Use the least amount of data necessary and the narrowest appropriate access.
- Do not send district data to personal email or store it in personal cloud accounts.
- Lock your screen whenever you step away.
- Do not photograph or post screens, badges, documents, workspaces, or student information.
- Dispose of printed sensitive information using approved secure methods.

FERPA AND PRIVACY	Student information must be handled only for legitimate educational or operational purposes and only through approved methods.

5. Secure devices, software, and connections

- Use district-managed devices and keep them physically secure.
- Install updates and restart when prompted. Updates often correct security weaknesses.
- Do not disable security tools or change protected settings.
- Do not install software, browser extensions, or mobile apps unless approved.
- Avoid unknown USB drives and accessories.
- Use trusted networks. Be cautious on public Wi-Fi and never leave a device unattended.
- Report lost, stolen, or damaged district equipment immediately.

6. Report quickly

Early reporting gives Information Technology the best opportunity to contain risk. You will not improve the situation by hiding a mistake or trying to investigate it yourself.

Contact IT immediately if you:

- Clicked a suspicious link, opened an unexpected attachment, or scanned a suspicious QR code.
- Entered your district password or MFA code on a site you now distrust.
- Approved an MFA request you did not initiate.
- Sent sensitive information to the wrong person or shared it too broadly.
- Notice unusual sign-ins, missing messages, sent mail you did not create, or unexpected account changes.
- Lose a district device, badge, security key, or phone used for authentication.
- Suspect malware, ransomware, unauthorized access, or another security incident.

1 STOP	2 REPORT	3 PRESERVE
Disconnect from the suspicious activity. Do not continue clicking or replying.	Call the IT Help Desk at 281-634-1300 and follow district reporting procedures.	Keep the message and note what happened. Do not delete evidence unless IT directs you.

District account resources

Password and recovery portal	https://my.fortbendisd.gov/
IT Help Desk	281-634-1300
Online support portal	https://help.fortbendisd.gov/
Get IT Help instantly 24/7/365	https://help.fortbendisd.gov/ava

Note: Additional guidance and expectations can be found on the Fort Bend ISD Employee Handbook, Resources - Fort Bend Independent School District

Quick knowledge check

1. An unexpected MFA prompt appears on your phone. What should you do?

2. A supervisor appears to request student data urgently by email. How should you verify the request?

3. You clicked a suspicious link but nothing happened. Should you report it?

4. Is it acceptable to reuse your district password on a personal website?