|  |  |
| --- | --- |
| **ITS CYBER NEWSLETTER OCTOBER 2024** | **AWARENESS IS THE KEY TO CYBERSECURITY** |



You are a target!

p

Sure, criminals can hack into your computers and accounts, but they know the easiest way to get access is to trick you into letting them in, and phishing is the most common way they do this. Over 3 billion phishing emails are sent each day! While the threat is real and relentless, you can help protect yourself by noting key areas in your email messages.

Look at the sample email message below to see some of the items you should focus on to help protect yourself from becoming a victim of a phishing attack.

# **FROM**

* Email is from an unknown address.
* You know the sender, but the email is unexpected or unusual.

# **TIME**

* You usually receive an email during work hours, but it was sent at an unusual time.

# **GREETING**

* Is the greeting unusual? Is it generic when it is usually personalized or vice versa?

# **HYPERLINKS**

* There are misspellings in the link.
* Email asks you to click a link.
* When you hover over the link, the address is for a different site.

From: [hr@browardschools.cnet](mailto:hr@browardschools.cnet)

To: [frank@browardschools.com](mailto:frank@browardschools.com)

Date: September 12, 2024 2:00 AM Subject: Urgent Notice

Hola Value Employee,

Now that our new CIO has been selected and starting soon, I’m asking everyone to complete this quick survey so we can identify who needs a new computer. It should take you only a few minutes but it must be completed by the end of the day or else you risk not getting a new computer.

Click here to take the [https://survey-monkee.com/] or download the attachment.

Thanks in advance for your cooperation! This really helps me out!

# Your Superintendent**SUBJECT**

* The subject line is generic or doesn’t match the content.
* Email is about something you never requested or is a receipt for something you never purchased.

# **CONTENT**

* The sender wants you to open an attachment.
* The email tries to instill panic or fear.
* You have an uncomfortable feeling, or the email seems odd.

# **ATTACHMENTS**

* Email has attachments you aren’t expecting (any attachments should be cautiously approached, even if you expect them).

Phishing scams can happen to anyone and aren’t always easy to spot. If something doesn’t feel right, pausing before responding is okay. Taking a few moments to breathe **O**.**U**.**T**. can help keep you safe.

**A red and white sign

Description automatically generatedO** – **O**bserve the sender. Do you know them? Were you expecting the email?

**U** – check **U**RLs (and email addresses). Is it spelled correctly? Is it coming from Gmail.com or some other online email service, not browardschools.com?

**T** – take your **T**ime. Look over the email for any red flags (like those noted in the sample email). Evaluate the message and what’s being asked of you. Does it make sense? Does it involve money or personal information that someone shouldn’t ask you for? Is the request just unusual? Hover over the sender’s name to see what address the message is coming from.

*Don't hesitate to contact a cybersecurity team member if you have any questions or want to learn more about cybersecurity.* [*ITSECURITY@BROWARDSCHOOLS.COM*](mailto:ITSECURITY@BROWARDSCHOOLS.COM)