IS THIS EMAIL DANGEROUS?

10 ways to help decipher if an email is safe

1. Is it asking you to take action?
Need to download attachment or click a link? Always, always, always call the person to verify!

2. Is there bad grammar/spelling?
Any professional company will have their emails proofed before going out to people.

3. Is the email addressed to you directly or "to whom it may concern"?
If it is too general be extra careful.

4. Is the sender's email address accurate?
Hackers can create fake email address very easily that look just like the real thing.

5. When you logged into your email, did it prompt you again?
If you already typed your password and a pop-up asks you to type it again—BEWARE!

6. A locked padlock symbol does not mean it is safe.
The padlock symbol indicates a secure channel, but not necessarily a safe site.

7. Were you shoulder surfed?
People can stand behind you in cafes, lines at stores, etc. and watch you type in your username and password.

8. Is there someone new in your organization?
Hackers watch press releases, websites, etc. to see who might be new to a company and take advantage of this.

9. Have you discussed a future purchase via email?
Hackers can read all of your emails and jump into a conversation, mimicking the other person.

10. Hover over any links or addresses in your email.
A hacker can type anything they want, but the actual link may be different.

See back for more detailed instructions of each item

2670 Lehigh St. Whitehall, PA 18052 610-264-1232 ezmicro.com

EZ MICRO SOLUTIONS

1. Is it asking you to take action?

Always, always, always call the person to verify! If they actually sent you something, they will tell you. Don't email—always verify verbally. If you are unfamiliar with the company, don't use the phone number listed in the email. Instead, google the company to verify it is an accurate phone number.

2. Is there bad grammar/spelling?

Any professional company will have their emails proofed before going out to people. If the email doesn't sound right, it probably isn't.

3. Is the email addressed to you directly?

If it is addressed to "whom it may concern" or any other group email name, be extra careful.

4. Are the reply to and from the same address?

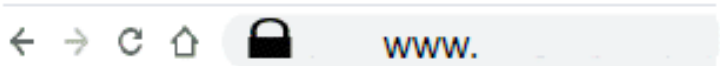
You might often correspond with Rachel@thatcompany.com, but if you received a message from Rachael@thatcompany.com, would you instantly spot the difference? For example, our emails come from ezmicro.com, but if you receive one from ezmicrosolutions.com, it would look real.

Another indicator would be the name in the "From" field. Does the "From" field contain a full email address or just the person's name? Hackers often type the real email address in the "From" field, but it actually came from a fake domain.

5. When you logged into your email, did it prompt you again?

When you logged into your email, was there another pop-up asking you to enter your password again? If you have already entered your password, DON'T enter it again. It could be a fake program that is grabbing your password. Most people use the same passwords and that gives the hackers access to many other accounts.

6. A locked padlock symbol does not mean it is safe.



The padlock symbol indicates a secure channel, but not necessarily a safe site. You might "securely" send someone your credentials.

7. Make sure you haven't been shoulder surfed recently!

People can stand behind you in cafes, lines at stores, etc. and watch you type in your username and password. Don't be surprised if they take it one step further and strike up a casual conversation with you and find out even more details!

8. Is there someone new in your organization?

Hackers watch press releases, websites, etc. to see who might be new to a company and take advantage of this. HR always sends out an email announcing new people so people let their guard down. Don't fall for it if they want you to click on a file to "look at their bio." Call HR to verify first!

9. Have you discussed a future purchase via email?

Hackers can read all of your emails and jump into a conversation, mimicking the other person.
For example, if you have been talking to your husband about a new washing machine you want to get, a hacker can send you a link that looks like it's from your spouse.

10. Did you hover over any links or addresses in the email to verify?

A hacker can type anything they want but the actual link may be different. For example, it might look like Dell.com, but if you hover your mouse over the Dell.com, you will see a different address altogether. What is printed should be the same as where you are going.

Example: