# Best practices to HALT HACKERS looking to exploit the pandemic

Cyber crooks want you to download their malware, and they'll try to trick you. A simple alert to IT could prevent big problems.

Do not open emails that:

- Report news related to COVID-19

- Masquerade as an alert from the World Health Organization

- Purport to come from a friend or colleague but seem unusual

- Catch you off guard in any way
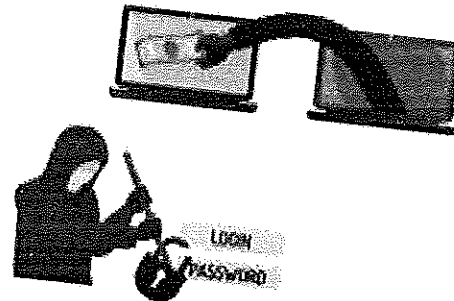
And *never* open an attachment or click a link if the sender is unknown

To immediately report any suspicious email, contact:

Watch what you click

During the global spread of the coronavirus, thousands of new phishing and scam websites have popped up with coronavirus-related buzzwords.

Adhere to telecommuting policies and procedures!

Remote access to organizational resources creates its own unique risks. Ensure information sent, particularly information containing protected health information, is encrypted.

Among safe practices:

- Encrypt whenever possible
- Don't share work devices
- Don't download information to personal devices
- Stay off public wi-fi
- Report lost or stolen devices immediately