Cybersmart SAFETY TIPS

Add these useful tips to your cybersmart arsenal to keep yourself and your organization safe!

PHISHING

Always verify email addresses and links, and be wary of unexpected attachments or urgent requests for sensitive information.

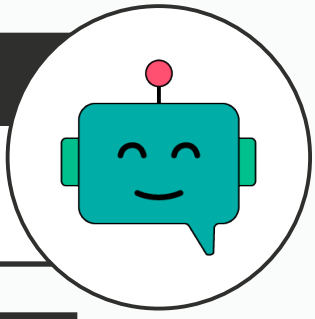
BUSINESS EMAIL COMPROMISE

Ensure all business communication is verified through known contacts and secure communication channels.

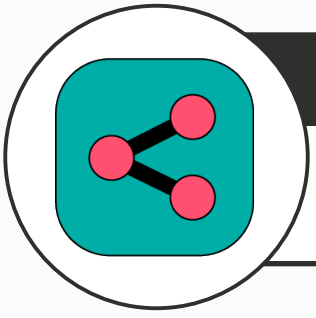
PRETEXTING

Verify the requester's identity through trusted communication channels before sharing sensitive information or complying with any unusual requests.

AI CHATBOTS



Follow your organization's policy regarding the use of AI chatbots. Never share any personal or organizational information with them.



SOCIAL MEDIA

Set strict privacy settings and be cautious about sharing personal information, location, or other sensitive details on social media platforms.

KnowBe4

Did you know over 80% of cyberattacks target individuals like you?

Phishing is when cybercriminals try to trick you into giving out sensitive information or taking a potentially dangerous action, like clicking on a link or downloading an infected attachment. They do this using emails disguised as contacts or organizations you trust so that you react without thinking first. Successful cyberattacks can result in financial harm, reputational damage, or data theft.

Remember the tips below to help against the dangers of phishing!

Do you know the sender?

Never reply to messages from unknown senders. If the sender claims to be from your organization, but you are unsure of their identity, contact them from a known phone number or email.

Did the message ask you to log in to an unusual website?

Always review links for misspellings or anything suspicious to make sure they are taking you to a trusted website before clicking on them.

Does the message make a strange, unusual, or urgent request? Does it bring out strong emotion?

This is a bad sign. Always think critically about the actions you are about to take. If you are unsure, contact your security team.

As always: stop, look, and think before taking any action!

Cybersecurity Skeptic No More!

I help protect my organization from cybercrime by keeping these tips in mind, and you can too!

Phishing Emails | Identify phishing emails

- Does the email come from an unknown sender, or is the email address misspelled?
- Does the email contain grammatical errors and misspelled words that are unusual from the sender?
- Does the message create a sense of urgency, such as stating that immediate action is required?
- Does the email include unexpected attachments or suspicious links?

Account Protection | Create strong passwords

- Create a memorable, complex password with at least 16-20 characters.
- Never reuse a password.
- Use an organization-approved password manager.

Websites and Links | Avoid clicking on malicious links

- Review them carefully. Cybercriminals may disguise, misspell, or add extra characters to the link to look like a trusted website.
- Search for the website's actual domain using a search engine like Google or Bing. When in doubt, don't click on the link.

Cybercriminals can target anyone, even you! If something seems suspicious, report it!

Remember these tips to protect yourself and your organization!

KnowBe4