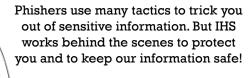


CYBERSECURITY 101

A National Cybersecurity Awareness Month message, brought to you by the Division of Information Security



How IHS Helps Prevent You From Getting Reeled In





It becomes a spearphishing attack when the crook targets you due to your affiliation with an organization. Sneaky spear phishers might even impersonate someone in your contacts list!

C'mon buddy! You can trust me!



Email campaigns are a popular method of phishing attacks.

Lucky for us, IHS has automatic spam filters that block much of the unwanted email before it gets to your mailbox.





But IHS is prepared to battle the threat with automatic virus scans on all attachments and downloads.



Another popular method of phishy exploitation is to convince you to download malware like keystroke-loggers or spyware onto your computer.



Hopefully you never click on a culprit link, but if you do, WebSense blocks network traffic to many known trouble spots. Often, phishing emails contain links to phony websites, and urgent messages to follow the link to resolve some problem.

Don't Take the Bait! Phishers Can be Foiled!



IHS works hard to protect its users and its patients from sensitive information breaches.

But IHS employees must be vigilant against social engineering too.

Hi! This is your IT Department. Can I have your account password?



Social engineers can call you too. They might even visit you in person!



Beware of anyone who asks you to disclose sensitive information!



