


National Cybersecurity Awareness Month

 National Cybersecurity
Awareness Month



OCTOBER 2018

WEEK 4

Safeguarding the Nation's Critical Infrastructure

Look out! The Evil Society of Cyber Hackers is on the loose! They are attacking Indian Health Service's critical infrastructure systems and are looking for vulnerabilities to exploit! Luckily, the heroic IHS Defenders are here to fight back and stop their evil plans! Both sides of this battle are highly skilled and very good at their jobs! Take a look at each side's super-effective habits below...

5 Habits of Highly Effective Hackers

With this malicious code, I, Major Malware, can infect the entire IHS hospital network!



Habit 1: Malware can be distributed in many ways – email attachments, drive-by downloads, compromised or malicious websites, and even pop-up windows. Get creative - the more evil, the better!

While you distracted them with your your malware, I snuck in and stole their data!



Excellent work, Root Kitty! Very evil!

Habit 2: Never have just one evil plan! Juggling multiple evil plans ensures success and chaos!

You're up, Phish Bait!



This clever email will look like it's from the CEO! That will convince them to give us the passwords we need!

Habit 3: A hacker's most effective ploy is phishing their victims with emails that seem to come from a legitimate source. A supervisor or trusted ally works best!

This user's passwords are simple and used on multiple accounts. With their Netflix password, we can now get into the hospital's patient data.



Excellent work, Bot!

Habit 4: Passwords are a critical defense for protecting online accounts, but victims often fail to make them strong ones. If you can crack one password, try to use it everywhere!

This is perfect! Captain Cybersecurity says on his social media that he's leaving town to...



Habit 5: The best victims share too much information online. Hunt through their social media accounts to find excellent tips on phishing ideas, password hints, and the best time to burglarize!

5 Habits of Highly Effective IHS Defenders

Thanks to that software update, we survived Malware's nefarious attack... but what does he have planned next?!



Habit 1: Installing updates allows software creators to "patch" security issues discovered in their products. Stay vigilant, heroes, and update patches as soon as they are released!

Good save, Big Backup! With everything backed up to a network server, we won't lose any data!



Habit 2: Executing regular backups ensures that you won't lose everything if your systems and data are ever infected. Regular backups ensure that you won't need to pay ransom to access your own data!

Don't open that email!



Always check the sender's address, hover over links, and think twice about unexpected attachments. Anything phishy? Call the sender or trash it!

Habit 3: Examining your emails closely makes it harder for clever phishers to trick you into compromising your systems and data.

It was close, but we used a passphrase to create a new unique password, and as long as the user changes it regularly, they won't get in.

Nice work, Strong Password! Now, we're leaving to...



Habit 4: Passphrases are easy to create and more difficult to crack. Turn a phrase into a password using the first letter of each word: "A Hero can be AnyONE, Even SomeONE Using Strong Passwords" = AHcb@1E\$1USP.

"...visit some old friends!" No! How did you find us?!



The homing beacon we embedded in the data we let you "steal" led us straight to you!

Habit 5: If you are vigilant and prepared, you will prevail against the forces of evil. Never let down your guard and always be on the lookout for clues that the bad guys are on the attack!

The IHS Defenders saved the day once again! But The Evil Society of Cyber Hackers will never stop! Will you be ready next time to be an IHS Defender? Never forget: how effective the Hackers are is entirely dependent on how effective a Defender you are! For questions, contact your local IT staff or cybersecurity@ihs.gov.