CYBER SHADOWS

The dark side of the cyber world that follows you around

THIS MONTH'S TOPICS:

There's no doubt that there is a dark side of the internet, but have you ever felt like it was following you around?

Scammers can lurk right behind every online step you take, developing specialized attacks geared towards individuals, and looking out for easy targets.

We don't want you to be scared of your online shadow, but we do want you to realize that it's always there, so that you can put the proper safeguards in place and respond accordingly.

The Shadows that Follow you on Social Media

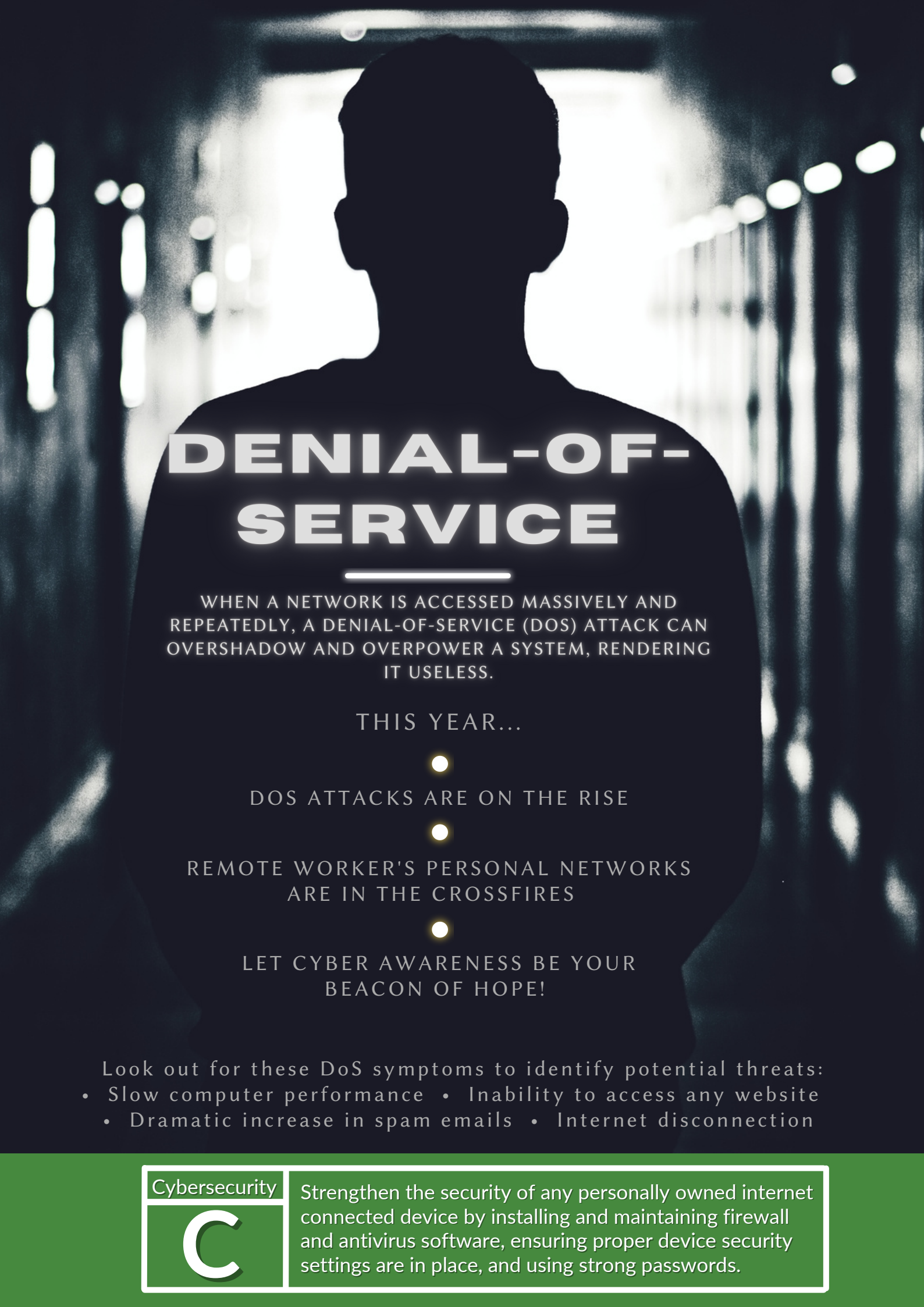
Scammers use the information you post against you. Oversharing can lead to disclosure of personal information, or hints to simple passwords such as your dog's name.

Shine light onto your profile

A lot of information can be gathered from selfies if a hacker just zooms in: Like info on a computer screen, or your specific location.

Hackers can gain access to unused accounts to perform nefarious activities, or gather PII.

- Take inventory and delete old accounts by using online resources, or searching for previous usernames.
- Review your photos and videos, foreground and background, before posting, and adjust your privacy settings to further increase security.
- Be honest about how much information you share on social media and how secure your friendship network is. Then check your account's privacy settings to make sure they coincide with your habits and security goals.



DENIAL-OF-SERVICE

WHEN A NETWORK IS ACCESSED MASSIVELY AND REPEATEDLY, A DENIAL-OF-SERVICE (DOS) ATTACK CAN OVERSHADOW AND OVERPOWER A SYSTEM, RENDERING IT USELESS.

THIS YEAR...

- DOS ATTACKS ARE ON THE RISE
- REMOTE WORKER'S PERSONAL NETWORKS ARE IN THE CROSSFIRES
- LET CYBER AWARENESS BE YOUR BEACON OF HOPE!

Look out for these DoS symptoms to identify potential threats:

- Slow computer performance
- Inability to access any website
- Dramatic increase in spam emails
- Internet disconnection

Cybersecurity	
C	Strengthen the security of any personally owned internet connected device by installing and maintaining firewall and antivirus software, ensuring proper device security settings are in place, and using strong passwords.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Peter practically lives on Social Media. It's so convenient to stay connected with friends and family, and he loves that he can easily access other websites by connecting to his social media account with the click of a button.

In his free time, Peter enjoys the quizzes and community building activities that circle the platform. Just this week, he joined in to wish this year's graduating seniors well by posting his own graduation picture with #CongratsGrads. And the week before, he discovered that his Hogwarts house was Gryffindor, along with 7 of his other friends who took the quiz.

Now, he's been tagged to do an "about me" challenge, to see if his friend's really know his favorite color, mother's maiden name, or his first car. But, when trying to sign in, he realized he's been blocked out. He also can't access several other accounts, including his social media, bank, and even work accounts. He's been hacked!

It's hard to pinpoint what activity led to the breach, but since Peter never took the time to adjust his privacy settings, nor come up with a unique password, anyone, including hackers, were free to lurk around his personal information and easily brute force their way into his account.

Did you spot the red flags?

- Peter never adjusted his privacy settings, allowing for hackers to view his personal information. His graduation post, for example, was not only easily searchable through the hashtag, but also included his picture with his school and year of graduation, which is often used as a credential.
- Peter had a weak password. He then, used his social media credentials for a quick sign-in to third-party sites. This is often a recipe for disaster.
- Oversharing tends to coincide with social media quizzes and challenges. Peter should have further considered the information he was disclosing before hitting "post."

Though not all social quizzes are maliciously gathering your personal information, it is smart to read a quiz's terms of service before playing so that you're aware of the type of information the company is collecting, and how it will be used.

It's also good to consider the kinds of questions a quiz is asking. Even simple ones like: where were you born, where did you go on your first flight, or who's your childhood best friend, are the exact same questions asked when setting up your accounts' security questions.

Only 44% of Americans utilize/take advantage of privacy settings on accounts.

At a minimum, best practice is to hide these key pieces of PII from public view on your social media accounts: your phone number, birth date, email address, and location.

Key Takeaways

Scammers are following our online actions a lot more closely than we may realize.

Whether they are in the shadows, lurking behind our clicks, or overshadowing and overwhelming our networks, they are always searching for the weakest point to infiltrate. Don't let that be you.

Privacy settings are everything:
If you've left your social media privacy settings on default, you may be sharing a lot more information than you're comfortable with. Be sure to make those adjustments now before it's too late.

Denial-of-Service incidents are increasing:
With more employees working at home, off of personal networks that have less securities put in place than in-office networks, it's important to be aware of what DoS is, its symptoms, and what you can do to protect yourself.

Social engineering on Social Media:
Be mindful of "fun" quizzes and challenges that encourage you to disclose your own personal information and broadcast it online.

Empathic Intelligence

The ability to be self-aware and socially-aware in order to understand what another person is experiencing.

How does this relate to cybersecurity?

When you put yourself in someone else's shoes, you gain the ability to understand how they think. When you put yourself in the shoes of a scammer, the information you gather can then be used to better protect yourself.

Now apply this concept to cyber-awareness.

The next time you go to post something on social media, put yourself in the shoes of a scammer: could the information you're about to post be used against you?

The next time you create a password: imagine you're a scammer, how quickly would you be able to crack that code?