Cyberattacks & Fake News:

The Digital Frontlines of War

Why war intensifies digital threats

Modern warfare extends beyond the battlefield. As the value of information increases, many countries use digital warfare to disrupt, spy upon, or sabotage their enemies.

Private hackers motivated by nationalism, politics, or financial gain are taking advantage of the situation, intensifying online threats for us all.

As these threats grow, it's vital to stay alert so that we can stay safe at home and at work.

Why would *you* be attacked?

- Attacks have the potential to spread **beyond their initial targets**, posing risks to unrelated devices and online platforms.
- Trusted news and media platforms frequently encounter threats that can jeopardize consumers' safety.
- Your **personal social media profiles** could be **compromised in order to spread misinformation** or **malicious software** to your colleagues, friends and followers.
- Different organizations face a variety of attacks; **as employees, we can become inadvertent digital targets.**

Protect your home network

Install **recommended operating system and security updates.** A notification on your computer or phone should indicate when these are available.

Add **two-factor authentication** to all of your social media accounts (Facebook, Linkedin, Twitter, etc.) and email accounts. If possible, add a backup email account as well.

Avoid **opening emails, text messages, and files that promise tempting content** such as **news coverage, exclusive photos, etc.** If it's not from an official source, don't click on it.

Protect our network

We've got internal network security covered, so there is nothing technical you need to do.

Beware of any emails that request your assistance with technical or financial matters.

Keep checking the sender’s email address; remember that this is the most crucial step in detecting a phish.

Fight fake news!

Rely on **legitimate sources such as government publications**, **trusted channels, and widely accepted news sites,** and refrain from forwarding fake news. This will help to maintain morale while keeping us safe:

- Keep in mind that most social media rumors are unreliable.
- Erroneous instructions and guidelines may be shared by people with no security role.

Reporting matters now more than ever

In wartime, reporting cyber attacks becomes crucial. You should immediately report:

- Any phishing attempts
- Blackmail messages
- A request to provide personal information, password, or access code
- A user who distributes suspicious messages on any platform