8 WAYS

TO STAY SECURE FOR

NATIONAL CYBERSECURITY AWARENESS MONTH

Whether you're at work, at home, or on the go, threats to cybersecurity and sensitive data can follow you. Our uber-connected world makes it more important than ever to know the threats and their potential consequences.

That's why this October as part of National Cybersecurity Awareness Month, we're taking the opportunity to share resources and information designed to help you make safe and informed choices when it comes to cybersecurity.

Explore this infographic to learn how the eight key cyber risks we'll be focusing on this month can show up in your daily life, both at work and at home, and what to do about them.

INCIDENT REPORTING

THE RISK:

Exposed sensitive data or malware infection left unreported leading to data breaches, fines, and the compromise of vital customer or personal information.

WHAT TO DO:

- Report any potential security/privacy incidents to the right authority.
- Be sure to tell your IT department, human resources manager, or your direct supervisor.

IDENTIFYING PERSONAL INFORMATION

THE RISK:

Sensitive information left exposed, even accidentally, compromising the wellbeing of customers or coworkers.

WHAT TO DO:

- Internalize our company's data privacy policies.
- Report potentially exposed private data when you see it.

IDENTIFYING MALWARE

THE RISK:

Infected networks grinding work to a halt and exposing sensitive information.

WHAT TO DO:

- Take all necessary steps, such as regular software updates, to keep malware off your work and home computers.
- Keep an eye out for signs of malware, like pop-ups, blue screens, and system slowdowns.

PHYSICAL SECURITY

THE RISK:

Scammers accessing personal data or company secrets via stolen laptops or other devices.

WHAT TO DO:

- Be on guard for suspicious actions wherever you encounter them, even in the non-cyberworld.
- Always seek independent verification that attempts to get information—or get into your workplace—are legitimate.

SAFE USE OF SOCIAL MEDIA

THE RISK:

Exposed company secrets and sensitive information or damage to our company or your personal reputation.

WHAT TO DO:

- Follow our guidelines on posting about company matters on social media.
- Take full responsibility for what you share and whom you share it with.

CLOUD COMPUTING

THE RISK:

Sensitive work or personal documents left exposed on an unsecured storage tool or made vulnerable after credentials were exposed.

WHAT TO DO:

- Take the time to understand our company guidelines on cloud storage use.
- Carefully choose what kinds of information you place "in the cloud" and create secure passwords for your personal cloud sites.

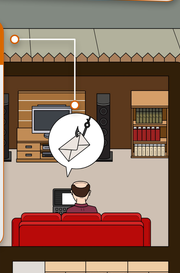
PHISHING AWARENESS

THE RISK:

Only one click on a phishing email or download of a suspicious attachment can lead to malware infection, data loss, and financial impacts.

WHAT TO DO:

- Scrutinize every email you receive for the signs of phishing (whether on mobile or desktop).
- Never click links or download files until you've taken the time to verify that they are safe.



WORKING/ COMPUTING REMOTELY

THE RISK:

Exposure of login credentials or credit card payment information due to an unsecured internet connection.

WHAT TO DO:

- Always look at websites to be sure they are secure (look for https://).
- Only use Wi-Fi networks that offer password protection.
- Use VPN connections to connect to work networks when working remotely.

Stay tuned later this month for more information on each of these risk areas.

Stay safe out there!