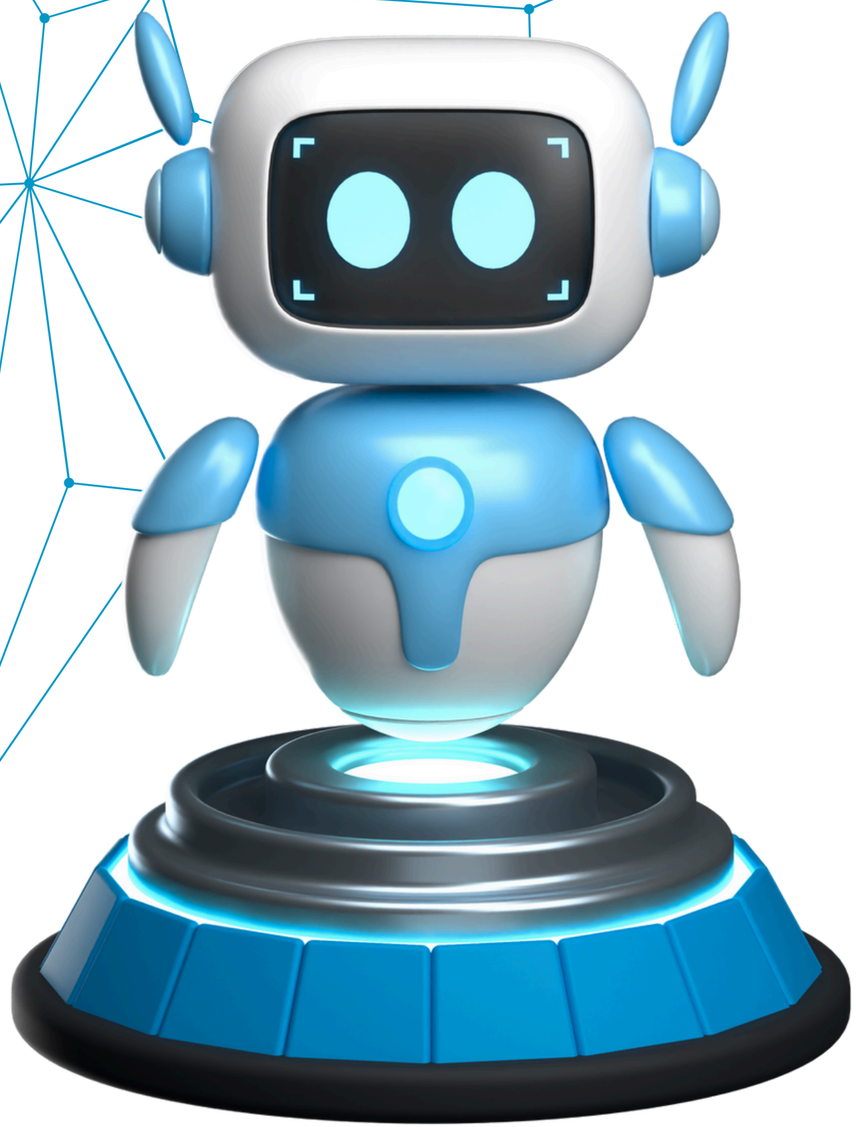
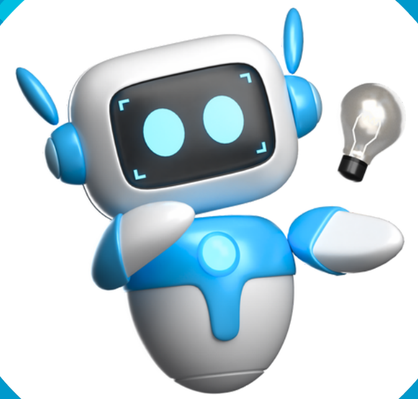


CYBERSECURITY AWARENESS MONTH

OCTOBER 2025

Guardians of the Firm:
Empowering Our Teams with Engaging Cybersecurity Tips

Objectives



For Cybersecurity Awareness Month, we are excited to introduce **"Guardians of the Firm: Empowering Our Teams with Engaging Cybersecurity Tips."** This campaign features a series of short, captivating social media-style videos designed specifically for legal professionals.

Our digital mascot will present key topics like phishing, data protection, and secure communication in a fun and relatable way.
Our goal is to educate, engage, and empower our teams to protect our digital assets, reduce cyber risks, and ensure regulatory compliance. The campaign will be shared across platforms to maximize reach and effectiveness, with success measured through engagement and feedback.

Problem Statement

In today’s digital age, legal professionals are increasingly targeted by sophisticated cyberthreats. Despite the critical importance of safeguarding sensitive client information and maintaining compliance with regulatory standards, many in the legal lack the necessary awareness and practices to effectively combat these risks.

This gap in cybersecurity knowledge and preparedness leaves the Firm vulnerable to data breaches, financial loss, and reputational damage.

Our Cybersecurity Awareness Month campaign aims to address this challenge by providing engaging, accessible, and practical cybersecurity tips to empower our teams to protect our Firm and our clients.

Campaign Overview

Campaign Concept: "Guardians of the Firm: Empowering Our Teams with Engaging Cybersecurity Tips"

Visual and Creative Approach:

- Theme: A dynamic duo – a Robot and an Firm employee working together as cybersecurity allies.
- Style: Fun, engaging, and educational social media-style videos that are easy to digest and memorable.

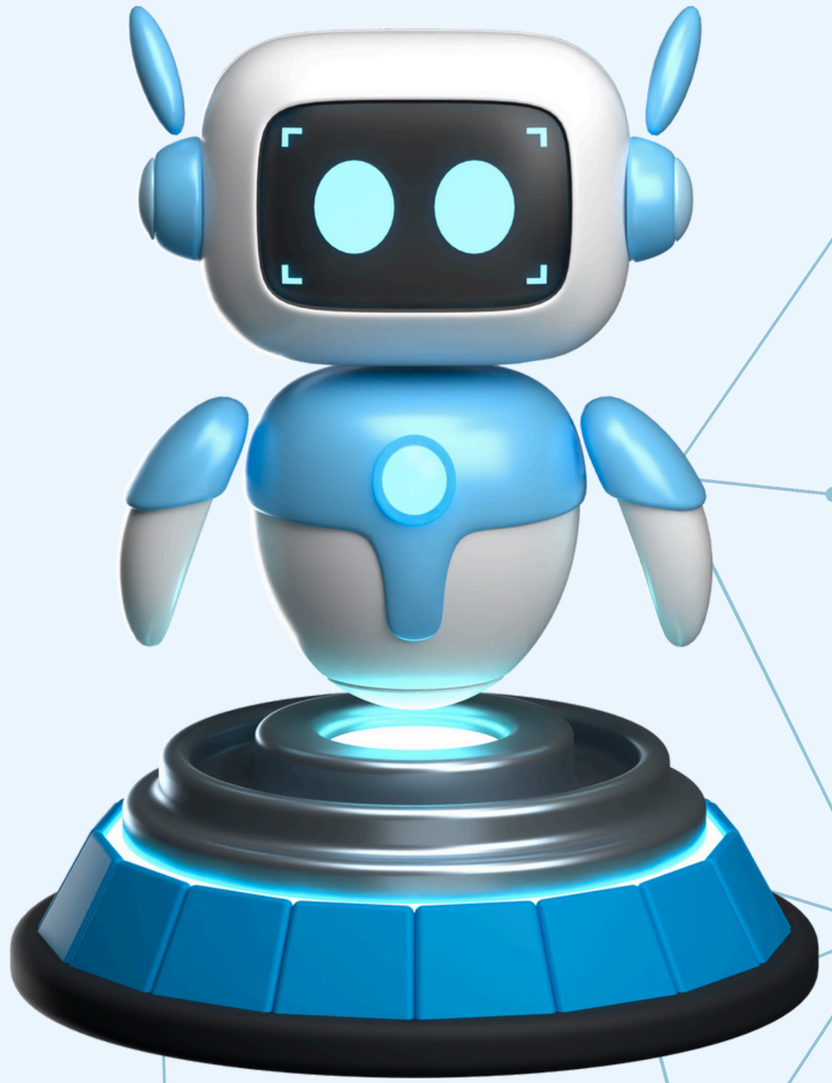
Campaign Elements:

- Characters:
  - The Robot: Represents advanced technology and cybersecurity knowledge.
  - The Employee: Represents our Firm professionals, eager to learn and protect the Firm.
- Content: Short, relatable videos that cover key cybersecurity topics such as phishing, data protection, and secure communication.
- Tone: Lighthearted and approachable, making complex cybersecurity concepts accessible and engaging for everyone.

Objective: To raise cybersecurity awareness and promote best practices among our teams, empowering them to protect the Firm's digital assets and ensure cybersecurity compliance.

Say Hello to Our Little Cybersecurity Friend!

Meet our new cybersecurity guardian, a friendly and vigilant robot designed to guide us throughthe best practices for keeping our digital environment safe. With a knack for spotting phishing attempts and a passion for strong passwords, this robot makes cybersecurity both engaging and easy to understand. Help us come up with the perfect name for our newest team member and join them on a journey to a more secure workplace!



Video Summaries

Phishing Trip: Don’t Take the Bait!

Video Concept:

An Employee at the Firm receives a suspicious email.
Just before opening it, the Robot appears like an angel on their shoulder and guides them: check the sender’s address, look for spelling errors, and avoid suspicious links.
By following the Robot’s advice, the Employee identifies the email as a phishing attempt and avoids a security breach.

Malware Minute: Don’t Get Infected!

Video Concept:

An Employee notices their computer running slower than usual. The Robot appears and explains what malware is, showing how easily it can infect a system. The Employee then demonstrates quick steps to avoid malware: updating software, not downloading unknown attachments, and using antivirus software.
Together, they emphasize the importance of staying vigilant against cyber threats.

Travel Smart: Mobile Security on the Go

Video Concept:

The Employee, preparing for a business trip, consults the Robot on mobile security while traveling. The Robot advises offers tips like avoiding free Wi-Fi and using a VPN for secure browsing, enabling device lock, keeping apps updated, and avoiding public charging stations.
By following these steps, the Employee ensures all devices remain secure throughout the journey.

Video Summaries

Laptop Lifesaver: Travel Tips for Security

Video Concept:

The Employee is preparing for a business trip. The Robot, eager to ensure security, suggests several important measures. A sports-style montage shows them doing tips like encrypting sensitive files, logging into a secure VPN connection instead of using public Wi-Fi, and taking their laptop with them when stepping away.
The Robot high-fives the Employee for a job well done as they take their laptop bag and jet off.

Deepfake Dangers: Spot the Impostor!

Video Concept:

The Employee encounters a strange video that gives them pause, and then the video gets glitchy. The Robot appears on the screen and explains how easily people can be impersonated with AI and what clues to look for. They offer tips on verifying identities, such as cross-checking information, using video calls for confirmation, and being cautious with sensitive information.
The Employee thanks the Robot for reassuring them about reality.

Windows Hello: Unlock Security with a Smile

Video Concept:

The Employee struggles to remember multiple passwords, often feeling frustrated and concerned about security. The Robot introduces Windows Hello, showing how it uses facial recognition to unlock devices effortlessly. With a simple smile, the Employee logs in securely, appreciating the convenience and enhanced protection.
The Employee grins, unlocking the Robot's heart.

Video Summaries

Dashlane Detective: Master Your Passwords

Video Concept:

The Employee fumbles with a stack of sticky notes covered in passwords. The Robot appears, "Let me introduce you to Dashlane.” Launching the app, "A password manager that creates strong passwords and securely autofills login details."
As the Robot demonstrates, the Employee watches in amazement.
"This is a game changer!" they exclaim.
The Robot nods, "No more sticky notes. Just secure, effortless logins."

Multi-Factor Magic: Secure Sharing Unveiled

Video Concept:

The Employee looks worried after hearing about a recent data breach. The Robot appears, "Multi-Factor Authentication (MFA) can add an extra layer of security. Let’s set it up."
They navigate through various accounts, enabling MFA step-by-step.
The Employee watches as the Robot demonstrates, understanding the additional protection it provides.
"Thanks for helping!" the Employee says. The Robot beeps, "With MFA, your accounts are much safer."

File Fortress: Share with Peace of Mind

Video Concept:

The Employee is about to send a confidential document via regular email. The Robot appears just in time.
"Let's discuss secure file sharing. Using encrypted email services or secure file-sharing platforms is much safer."
The Robot shows how to use these services, highlighting their benefits.
The Employee nods, impressed. "Got it! No more unsecure emails." The Robot beeps, "That's the way to keep information protected."

Video Summaries

Backup Buddy:
Protect Your Data

Video Concept:

The Employee panics as their computer crashes unexpectedly. The Robot appears, guiding them to set up automated backups.
"Regular backups are crucial," the Robot explains, "to protect your data from cyber incidents."
As the setup completes, the Employee feels a wave of relief, now understanding how vital these backups are in safeguarding their valuable information.

Web Wise:
Spotting Secure Sites

Video Concept:

The Employee prepares to access a client's confidential information online. The Robot appears, pointing out the missing padlock icon and HTTPS.
"Always check for these signs," the Robot advises, "to ensure a secure website."
The Employee nods, grateful for the tip. Now equipped to identify secure sites, they confidently protect their clients' sensitive data.

Password Power:
Create Invincible Keys

Video Concept:

The Employee sighs in frustration, staring at a list of compromised accounts. The Robot appears, ready to help.
"Let’s talk password creation. Use unique passwords for each account and avoid common phrases. Mix characters for strength."
The Employee updates their passwords. They thank the Robot, "I guess I'll need to write these down somewhere safe!" The Robot responds with a friendly beep.

Video Summaries

Wi-Fi Woes:
Stay Safe in Public

Video Concept:

The Employee encounters a security threat while using public Wi-Fi at a café and turns to the Robot for help. The Robot educates the Employee on the risks of using public networks and provides key safety tips: using a VPN, avoiding sensitive transactions, turning off file sharing, and sticking to secure websites.
The Employee follows the advice, successfully securing their connection and continuing their work with confidence.

Email Armor:
Encrypt Your Messages

Video Concept:

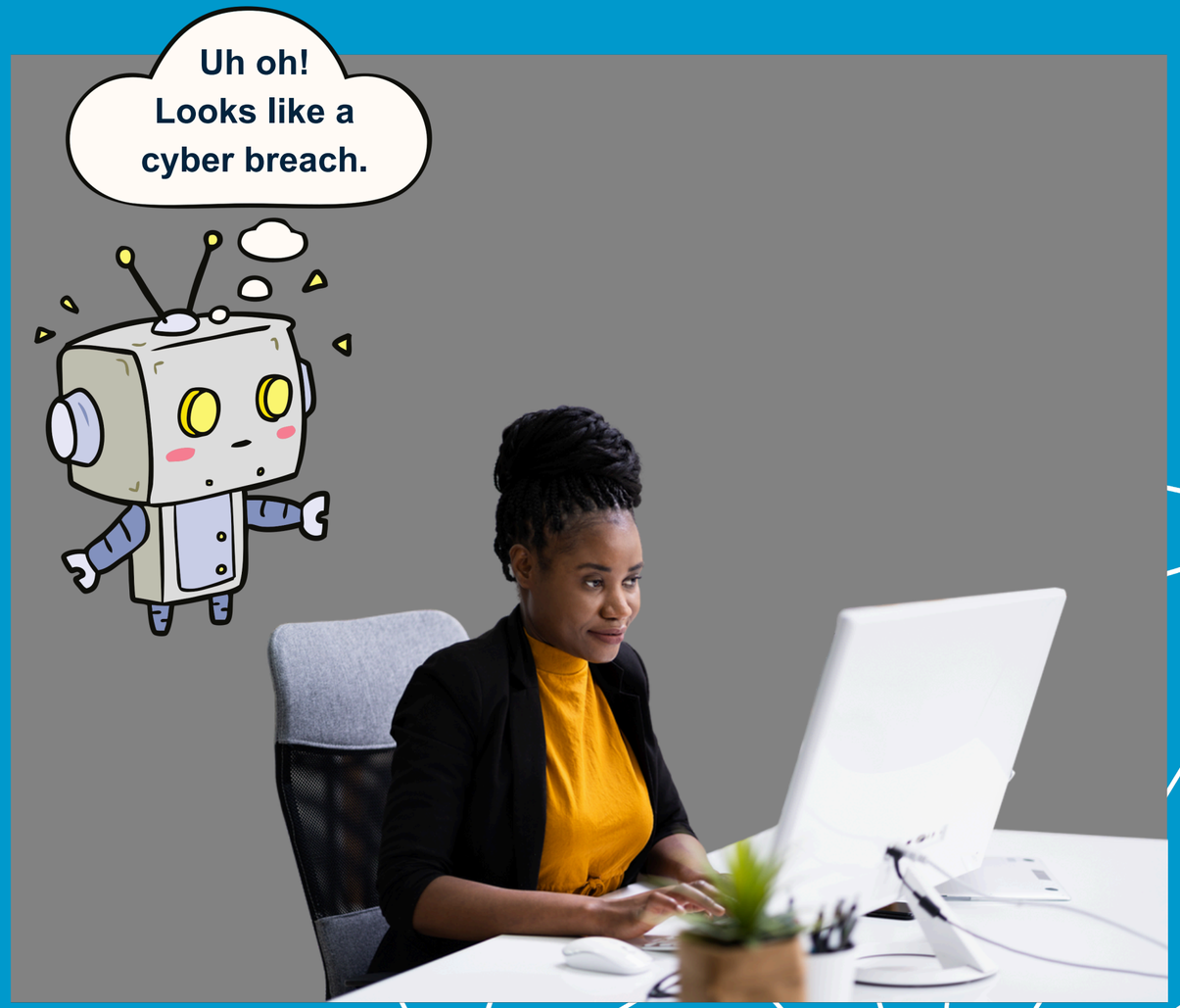
The Employee learns about the risks of unencrypted emails when the Robot explains how easily sensitive information can be intercepted. The Robot shows how encryption works like invisible ink, and guides the Employee through the process.
The Robot highlights the importance of secure communication, leaving the Employee confident and amused by the thought of hackers squinting at invisible ink.

Crisis Control:
Responding to Cyber Threats

Video Concept:

The Employee's computer screen flickers with unusual activity. Suddenly, the Robot appears.
"A breach is happening. Report it immediately and disconnect from the network."
The Employee quickly follows the steps. The Robot adds, "In the digital world, your quick response is your best defense."
The screen returns to normal, leaving the Employee relieved.

Visual Inspiration



Project Timeline

Phase 1: Presenting and Refining the Pitch

- Review and refine the pitch deck with the team
- Develop a detailed project plan and assign tasks to team members

Phase 2: Content Development and Finalization

- Consult with all necessary team members to develop quick tips and ensure accuracy
- Script and start storyboarding video content

Phase 3: Production and Shooting

- Gather and organize necessary elements for each video
  Scout out shooting locations
  Begin shooting and editing video content

Phase 4: Video Review and Finalization

Complete video editing and finalize all content
Gather feedback from key stakeholders and make necessary revisions

Phase 5: Final Preparations

- Ensure all internal channels are ready for content distribution
- Plan out scheduling
- Release teaser content to generate excitement
- Conduct a final check of all materials and platforms

Phase 6: Campaign Launch

- Release the first set of video content across all internal channels
- Send out the initial email campaign with key messages and resources
- Monitor engagement and gather initial feedback
- Address any immediate issues and ensure smooth operation

Phase 7: Post-Campaign Review and Follow-Up

Share success stories and positive feedback
Conduct surveys to gather feedback and measure engagement
Analyze metrics and evaluate the success of the campaign
Compile a report with key findings and insights
Plan for future cybersecurity initiatives based on feedback and results
Keep the conversation about cybersecurity alive through regular updates and tips
Continue to share relevant content periodically to reinforce key messages

THANK YOU!

We look forward to an effective and impactful Cybersecurity Awareness Month

CYBERSECURITY
AWARENESS MONTH
OCTOBER 2025