Certified Energy Expert

CYBERSECURITY AWARENESS

Resources to Stay Safe and Secure

YOUR DIGITAL IDENTITY IS VALUABLE.

Check if you've been breached:

- Visit **haveibeenpwned.com** and enter your email address to see if it's been involved in any known data breaches.
- Review **all affected platforms** and what type of information was exposed. Promptly **change passwords** and **monitor accounts** for suspicious activity.
- Sign up for notifications to **stay informed** of future incidents.
- Regularly check all email addresses to **stay on top of breaches** and **protect your digital identity**.

Have I Been Pwned

DEFENSE IN DEPTH

Passwords alone aren't enough.

No single defense is foolproof, which is why security works best in layers. Just as a castle has a moat, drawbridge, high walls, and guards, you should employ multiple defenses to keep your digital identity safe.

- Create **strong, unique passwords** for each account. Use **password managers** (we recommend Bitwarden, Lastpass, or 1Password) to securely store them.
- Enable **multifactor authentication** (MFA) on all your accounts. Prefer app-based MFA over SMS or email.
- Keep **social media private**. Don't accept **unknown friend requests** and don't share **sensitive information**.
- Secure devices by keeping them **up to date** and changing **default passwords**. Place smart devices on their own networks when possible.
- Avoid using public Wi-Fi when possible; use a VPN if you must connect.
- Practice strong physical security by enabling **auto-lock** and **tracking** features on your devices.
- Don't leave devices **unattended** in public spaces or in vehicles. Watch for "**shoulder surfing**" in shared spaces.
- Share best practices and tips with friends and family to stay safe and secure all year long!

RESPOND TO THREATS

Know what to do if you've been breached.

- **Identify** unusual activity, unauthorized charges, suspicious logins
- **Contain** by changing passwords, remediating affected devices, and employing other defense measures
- **Notify** proper authorities: banks, law enforcement, FBI
- **Monitor** accounts to prevent future incidents

RESOURCES

Report Fraud: reportfraud.ftc.gov

Internet Crime Complaint Center (IC3): complaint.ic3.gov

Identity Theft: identitytheft.gov

Check your passwords: haveibeenpwned.com

Freeze Your Credit:

Equifax: equifax.com | (888) 298-0045

Experian: experian.com | 888-397-3742

TransUnion: transunion.com | (800) 916-8800

BY YOU FOR YOU
2026 CEE NATIONAL MEETING

THE PINK PANTHER™ & © 1964-2024 Metro-Goldwyn-Mayer Studios Inc. All Rights Reserved.
The Color PINK is a registered trademark of Owens Corning. © 2024 Owens Corning. All Rights Reserved.

Certified Energy Expert

CYBERSECURITY IN THE AGE OF AI

Resources to Stay Safe and Secure

SAFE USE OF PUBLIC AI TOOLS

Publicly available AI tools can improve productivity, but they also introduce business, legal, and security risks.

1. Protect Confidential Information

- Do not enter confidential or non-public information into public AI tools. This includes proprietary business data, system details, financial information, customer data, or personal information. Share only minimal, non-identifying details.

2. Avoid Business or Technical Problem-Solving

- Do not use public AI tools to troubleshoot technical issues, analyze company data, or solve internal business problems. Detailed questions can unintentionally expose sensitive information and create security or compliance risks.

4. Be Careful What You Ask

- Questions alone can reveal non-public information. AI platforms learn from prompts and usage patterns, and shared information may be stored, analyzed, sold, or used to improve the system.

5. Assume Anything You Share Is Public

- Treat public AI tools like a public forum. If you wouldn't post it on a public website, don't enter it into an open AI system.

AI IN SAAS PLATFORMS

Many Software as a Service (SaaS) platform providers are using AI. Consider some questions to ensure transparency, data privacy, and ethical use:

Data Usage and Privacy	How is customer data stored, secured, and protected? (Consider data privacy regulations.)
Transparency	Can the vendor explain how their AI algorithms work in simple terms?
Consent and User Control	How is user consent obtained for collecting and processing data with AI, and can they opt out?
Bias and Fairness	How does the vendor address biases in their AI algorithms?
Security Measures	What security measures are there to prevent unauthorized access or breaches?
Compliance and Standards	Does the vendor adhere to industry standards for AI development and deployment?
Data Ownership and Portability	Who owns the data processed by the AI, and what happens if the customer ends the service?
Support and Accountability	What kind of support is provided in case of AI-related issues or incidents?

CYBERSECURITY THREATS IN THE AGE OF AI

Hackers are constantly finding new ways to exploit technology for malicious purposes.

THREAT		ACTION
Phishing Attacks	Hackers use generative AI to craft convincing phishing emails.	• Be skeptical of unsolicited communications • Don't click on links/download attachments from unknown sources • Verify sender address
Deepfakes	Generative AI enables videos, images, and audio where a person's likeness can be convincingly manipulated.	• Cross-check facts from reliable sources before believing or sharing any content. If faces and hands of people in images are distorted, it most likely was AI generated.
Social Engineering Attacks	Hackers can mimic the writing style of an individual to craft targeted messages, making it seem like the communication is coming from a trusted source.	• Be mindful of the information you share online.
Automated Password Attacks	AI algorithms can generate and test massive numbers of password combinations rapidly for brute force attacks, where hackers can crack weak passwords and gain access to user accounts.	• Monitor your accounts regularly • Use multi-factor authentication (MFA) and/or biometrics • Disable unnecessary permissions • Update passwords and use unique combinations
Sophisticated Cyber Attacks	AI-powered tools can be used by cybercriminals to launch highly sophisticated and targeted attacks by studying human behavior and exploiting individual vulnerabilities.	• Keep devices, operating systems, and applications up-to-date; • Use cybersecurity principles in every stage of AI, from data collection to deployment.
Data Privacy Concerns	Breaches in AI databases can result in identity theft, financial fraud, and other privacy-related crimes.	• Know your intellectual property • Have non-disclosure agreements (NDAs) in place • AI apps and devices to make sure they clearly state how your data will be collected, stored, and used • Choose reputable products and services