Asurtec

AN ASURTEC EXPERT SERIES

STAY SAFE BY UNCOVERING AI SCAMS

Learn how to **protect your organization** from the latest AI-driven threats.

Scan me

asurtec.com

TABLE OF CONTENTS

AI is transforming the world in unprecedented ways, bringing both incredible innovation and significant risks. Scammers are exploiting advanced technology—from fake celebrity endorsements to cloned human voices—to deceive and harm.

This ebook examines how AI-generated fakes are reshaping the landscape of fraud and provides actionable strategies to help organizations protect themselves from these emerging threats.

CHAPTER 1

THE GROWING THREAT OF VOICE CLONING

Don't get fooled: a familiar voice isn’t always trustworthy.

THE SOUND OF DECEPTION

Imagine receiving a call from your CEO for an urgent wire transfer. It sounds just like them—but it’s not. AI-powered voice cloning mimics someone’s voice with just seconds of audio, making fraud more convincing than ever.

THE RISKS

Financial losses and reputational harm from impersonation.

HOW TO PROTECT YOURSELF

- **Multi-Step Verification:** Require email confirmation, two-factor authentication (2FA), or a second internal approval.
- **Training and Awareness:** Educate your team about voice cloning and stay skeptical of urgent, unusual requests.
- **Call-Back Procedures:** Verify sensitive requests by calling back on known numbers.

CHAPTER 2

THE RISE OF DEEPFAKE VIDEOS

SEEING IS NO LONGER BELIEVING

AI-generated deepfake videos can create realistic footage of people saying or doing things they never did. Imagine receiving a video from your CEO endorsing a new product—it looks authentic, but it's a scam.

THE RISKS

- **Undermined trust** and damaged reputations.
- **Financial losses** from manipulated visual content.

HOW TO PROTECT YOURSELF

- **Public Awareness:** Educate your team about deepfakes so they can recognize and question manipulated content.
- **Multi-Channel Verification:** Confirm sensitive information through secure channels like direct calls or trusted internal messaging systems.
- **Vigilance:** Stay informed and implement strong verification protocols.

> Deepfake technology is now used to fake endorsements, manipulate opinions, and carry out extortion schemes.

CHAPTER 3

AI-GENERATED PHISHING EMAILS

PHISHING EMAILS REIMAGINED

AI has elevated phishing scams to a new level of sophistication. These emails mimic the tone, style, and language of trusted colleagues, supervisors, or Executive Directors (EDs). making them harder to detect than ever before.

THE RISKS

- Confidential **data breaches**.
- Financial losses and potential **ransomware attacks**.

HOW TO PROTECT YOURSELF

- **Email Authentication Protocols:** Implement SPF, DKIM, and DMARC standards.
- **Employee Awareness Training:** Train employees to spot phishing attempts, even subtle or personalized ones.
- **Multi-Factor Authentication:** Add an extra layer of security for all accounts.
- **E-mail security products** to catch and quarantine unwanted and dangerous mail."

AI-powered phishing evolves faster than your defenses—stay ahead.

CHAPTER 4

UNMASKING SYNTHETIC IDENTITIES

AI can fake an identity, but it shouldn’t fool your organization.

AI-generated synthetic identities—blending real and fake information—pose a serious risk to organizations handling confidential data. These scams lead to data breaches, compliance violations, reputational damage, and financial losses. Traditional background checks are no longer enough. Strengthening identity verification and access controls is critical.

HOW TO PROTECT YOURSELF

- **Use AI-powered identity verification:** Combine biometric authentication with standard background checks.
- **Monitor for suspicious activity:** Track irregular access to sensitive files or unusual login patterns.
- **Limit data access:** Ensure only authorized personnel can handle confidential information.
- **Conduct routine audits:** Regularly review and verify data usage.

By implementing these safeguards, organizations can stay ahead of evolving AI-driven fraud.

Want to learn more? Contact us today!

CHAPTER 5

WINNING THE WAR ON AI FRAUD

Your organization's security starts with an engaged and prepared team.

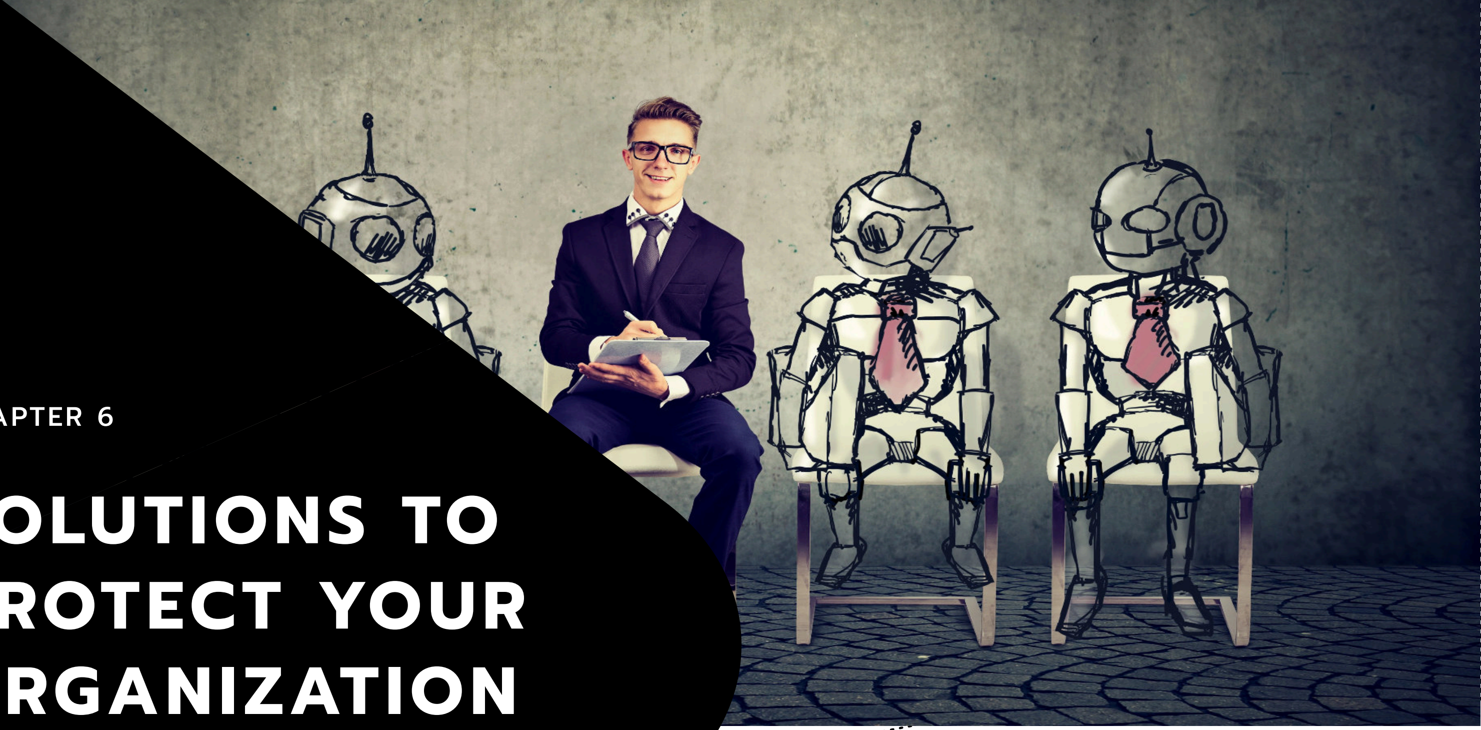
HOW TO STAY AHEAD

AI scams are evolving, becoming increasingly sophisticated. Organizations can stay ahead by building a culture of awareness where verification becomes second nature.

KEY STEPS TO TAKE

- **Train Your Team:** Educate employees to recognize manipulation and phishing attempts while adhering to verification protocols.
- **Trust but Verify:** Encourage employees to verify unusual requests or changes to financial details.
- **Empower Employees:** Provide tools like email authentication and liveness detection to support secure decision-making.
- **Promote Reporting:** Foster a safe and judgment-free environment for reporting suspicious activities.
- **Reinforce Accountability:** Make cybersecurity a shared responsibility at all organizational levels.

Prepared teams are your strongest defense. Build a culture of awareness and verification. We can help!



CHAPTER 6

SOLUTIONS TO PROTECT YOUR ORGANIZATION

KEY STEPS TO STRENGTHEN YOUR DEFENSES

- **Multi-Layered Verification:** Use MFA and approval workflows to secure access.
- **Liveness Detection:** Confirm real-time presence during key interactions.
- **Secure Communication Channels:** Protect sensitive data with encryption.
- **Cross-Channel Validation:** Verify requests through multiple trusted methods.
- **Employee Training:** Equip teams to spot and respond to threats effectively.

BUILDING UNSHAKABLE DEFENSES

By embedding these strategies into daily operations, organizations can stay ahead of even the most convincing AI-driven scams. Combining awareness, verification protocols, and technology, you can protect your business from financial and reputational harm.

Proactive measures today prevent disasters tomorrow.

BUILDING CYBER CONFIDENCE FOR YOUR TEAM

"

Cybersecurity isn't just about technology—it's about people. With over 35 years in non-profits, I can help your team build the skills they need to spot and prevent modern threats like social engineering, ransomware, and password vulnerabilities. Together, we'll create a safer and more secure organization.

I've designed a comprehensive cybersecurity training program tailored for community organizations. Together, let's equip your team to stay ahead of cyber risks.

"

Cathy Timlin
Asurtec Cybersecurity Trainer

Asurtec

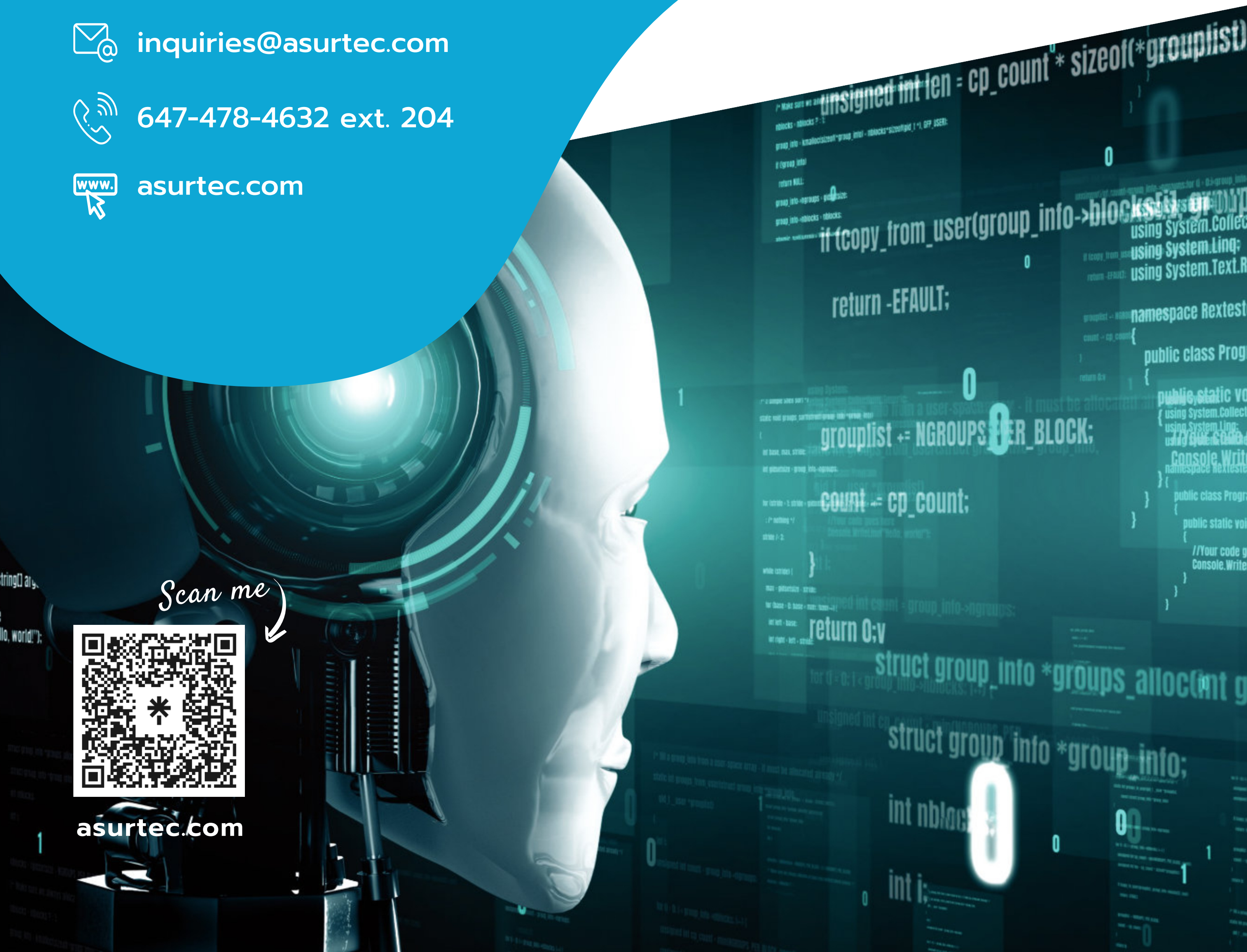
SUPPORT AND RESOURCES

Contact Asurtec for personalized advice and advanced cybersecurity solutions tailored to your organization's needs.

✉ inquiries@asurtec.com

☎ 647-478-4632 ext. 204

www. asurtec.com



Scan me

asurtec.com