Upper Albany Main Street

TECHNOLOGY NEWSLETTER

MID-2026

Innovate. Connect. Grow.

MID 2026

Upper Albany Main Street

CYBERSECURITY IN 2026



PROTECT YOUR BUSINESS. PROTECT YOUR FUTURE.

Cyber threats are increasing—and small businesses are often the target. Simple steps today can protect your data, your customers, and your reputation.

SECURITY IS EVERYONE'S JOB

Every employee plays a role in keeping your business safe and secure.

WHY IT MATTERS

THREATS ARE REAL

Hackers use smarter tools every day to steal data and disrupt businesses.

YOUR DATA IS VALUABLE

Customer information, financial data, and business files are worth protecting.

MISTAKES HAPPEN

One email click or wrong link can lead to big problems.

YOUR REPUTATION COUNTS

A security breach can damage trust and cause long-term harm to your business.

5 SIMPLE WAYS TO STAY SAFE

1. **Use Strong Passwords**
   Create long, unique passwords and change them regularly.
2. **Be Careful with Emails**
   Don't click on links or open attachments from people you don't know.
3. **Keep Software Updated**
   Updates fix security problems. Turn on automatic updates.
4. **Lock It Down**
   Lock your screen and secure your devices when away.
5. **Speak Up**
   Report anything suspicious to your team right away.

HOW UAMS CAN HELP

Upper Albany Main Street offers training, tools, and resources to help business owners stay safe online.

- Cybersecurity Basics for Business Owners
- Employee Awareness Training
- Phishing & Scam Prevention
- Data Protection Best Practices
- Free Resources & Local Support

We're here to help you protect what matters most.

Cybersecurity doesn't have to be complicated.
TOGETHER, WE CAN BUILD A SAFER, STRONGER COMMUNITY.

AI FOR SMALL BUSINESS

SIMPLE TOOLS. SMARTER WORK. BIGGER OPPORTUNITIES.

Discover how Artificial Intelligence can help you save time, attract customers, and grow your business.

1 WHAT IS AI?

Artificial Intelligence (AI) is technology that helps businesses complete everyday tasks faster and more efficiently.



- Write emails and social media posts
- Create flyers and marketing materials
- Answer customer questions faster
- Organize information and documents
- Brainstorm new business ideas
- Save time on repetitive tasks

2 WHY BUSINESS OWNERS USE AI

SAVE TIME
Spend less time on paperwork and routine tasks.

CREATE CONTENT FASTER
Generate emails, flyers, social media posts, and ads in seconds.

IMPROVE CUSTOMER SERVICE
Respond to customers faster and provide better experiences.

MAKE BETTER DECISIONS
Analyze information quickly and organize your ideas more effectively.

3 AI CAN HELP BUSINESSES LIKE YOURS

RESTAURANTS
- Create menus
- Write social media posts
- Respond to customer reviews

RETAIL STORES
- Product descriptions
- Marketing campaigns
- Customer emails

SERVICE BUSINESSES
- Appointment reminders
- Marketing materials
- Customer communications

NONPROFITS
- Grant writing assistance
- Event promotion
- Reports and presentations

4 USING AI RESPONSIBLY



- Review AI-generated information before using it
- Protect confidential business information
- Use AI as a helper—not a replacement for your expertise
- Continue learning as technology changes

5 HOW AI CAN HELP YOUR BUSINESS GROW



AI can help you work smarter, serve your customers better, and find new opportunities. Start small, stay curious, and watch your business grow.

- Save time and work smarter
- Boost productivity
- Attract and engage customers
- Improve communication
- Make better decisions
- Drive business growth



READY TO LEARN MORE?

Explore how AI can help your business save time, reach more customers, and grow with confidence.

COMPLIANCE
IN THE DIGITAL AGE



A RESPONSIBILITY. A PRIORITY. A COMPETITIVE ADVANTAGE.

As a business owner, protecting your information, your customers, and your reputation is essential. Compliance helps you reduce risk, build trust, and meet legal and industry standards—so you can focus on growing your business with confidence.

HOW BUSINESS OWNERS CAN BE COMPLIANT

Protect Customer Data
Safeguard personal, financial, and business information with strong privacy practices and secure systems.

Secure Your Information
Use strong passwords, encryption, and access controls to prevent data breaches and unauthorized access.

Keep Accurate Records
Maintain organized, up-to-date records in accordance with legal, tax, and industry requirements.

Communicate Transparently
Share clear policies with your team and customers. Be open about how you collect, use, and protect data.

Follow Laws and Regulations
Understand and comply with applicable laws and industry standards that apply to your business.

SMART PRACTICES FOR TODAY'S BUSINESS OWNERS

Limit Access
Give access to sensitive information only to those who need it.

Use Strong Passwords
Require strong, unique passwords and change them regularly.

Back Up Your Data
Regularly back up important data and store it securely.

Train Your Team
Educate employees on security best practices and compliance responsibilities.

Review and Update Regularly
Review your policies, procedures, and systems often to stay current with evolving risks and regulations.

WHY IT MATTERS

Compliance is more than avoiding fines—it's about building a stronger, more trusted, and more resilient business.

- It protects your business and your customers.
- It helps you avoid costly penalties and disruptions.
- It builds trust and strengthens your reputation.

EMAIL SECURITY

PREVENTING PHISHING & HACKS IN 2026



Cyber attackers are getting smarter—
and **email is still their #1 way in.**
Staying alert and following best practices
helps protect your information,
your business, and your reputation.

WHAT IS PHISHING?

Phishing is a trick used by cybercriminals to steal your information or gain access to your accounts. It often looks like a real email from someone you know or trust.

WHY IT MATTERS

- Phishing attacks continue to rise every year
- One click can lead to stolen data, financial loss, or system downtime
- Protecting your email protects your business, your customers, and your reputation

HOW TO SPOT A PHISHING EMAIL

CHECK THE SENDER

Look closely at the email address. Attackers use fake or look-alike addresses.

WATCH FOR SUSPICIOUS LINKS & ATTACHMENTS

Don't click on links or open attachments unless you were expecting them.

LOOK FOR RED FLAGS

Urgent or threatening language, requests for personal information, or unexpected requests for money or gifts.

CHECK SPELLING & GRAMMAR

Poor spelling or grammar can be a sign of a phishing attempt.

VERIFY BEFORE YOU ACT

If something seems off, contact the sender using a known phone number or email address.

BEST PRACTICES

- Use strong, unique passwords and change them regularly
- Enable Multi-Factor Authentication (MFA) on all accounts
- Keep software and devices up to date
- Never share your login information
- Lock your screen when stepping away
- Think before you click!

Be smart. Be cautious. Be secure.

WHAT TO DO IF YOU SUSPECT A PHISH

1. Don't click. Don't reply. Don't open attachments.
2. Report the email using your email provider's report phishing feature.
3. Delete the email from your inbox.
4. If you clicked a link or entered information, change your password immediately. Consider enabling MFA if available.

**SECURE EMAIL. PROTECT YOUR BUSINESS.
SAFE COMMUNICATION. STRONGER FUTURE.**

Your awareness is your best defense.
Let's keep your business secure in 2026 and beyond!

TYPES OF CYBER CRIMES, ATTACKS & HACKS



Cybercriminals use many tactics to steal data, money, and disrupt operations. Know the threats so we can stop them together.

COMMON CYBER CRIMES, ATTACKS & HACKS

PHISHING

Fraudulent emails or messages designed to trick you into giving up sensitive information.

HOW IT WORKS

- Attackers impersonate trusted sources.
- You may be asked to click a link, open an attachment, or enter login details.
- Can lead to identity theft or account takeover.

MALWARE (VIRUSES, TROJANS, SPYWARE)

Malicious software installed on your device to steal, damage, or disrupt data.

HOW IT WORKS

- Delivered via email attachments, malicious downloads, or infected websites.
- Can steal data, monitor activity, or lock systems.

RANSOMWARE

Locks your files or systems and demands payment (ransom) to restore access.

HOW IT WORKS

- Often delivered through phishing or vulnerable systems.
- Encrypts files and displays a ransom demand.
- Can cause major downtime and data loss.

SMISHING & VISHING

Phishing attacks delivered via text messages (smishing) or phone calls (vishing).

HOW IT WORKS

- Urgent messages or calls create fear or pressure.
- You may be tricked into clicking links, sharing codes, or sending money.

PASSWORD ATTACKS

Attempts to gain access to accounts by guessing, stealing, or brute-forcing passwords.

HOW IT WORKS

- Uses stolen credentials, weak passwords, or automated tools.
- Leads to unauthorized access to email, systems, and sensitive data.

MAN-IN-THE-MIDDLE (MITM) ATTACKS

Attackers intercept and possibly alter communication

HOW IT WORKS

- Occurs on unsecured Wi-Fi or fake websites.
- Can steal logins, payment info, or confidential conversations.

SOCIAL ENGINEERING

Manipulates people into breaking security procedures or sharing confidential information.

HOW IT WORKS

- Attackers build trust or exploit emotions.
- May pose as IT, a vendor, or a coworker.
- Relies on human error, not technical hacking.

DDoS ATTACKS

Overwhelms websites or servers with massive traffic, causing outages.

HOW IT WORKS

- Uses many compromised devices to flood a target system.
- Disrupts online services and productivity.

STAY SAFE. STAY SECURE.

Be Alert

Verify unexpected emails, links, and requests—especially those asking for urgent action.

Use Strong Passwords

Create long, unique passwords and enable Multi-Factor Authentication (MFA) whenever possible.

Keep Systems Updated

Regular updates close security gaps and protect against known threats.

Think Before You Click

Don't click on suspicious links or open unknown attachments.

Protect Information

Share sensitive data only through approved, secure channels.

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY.

Together, we can protect our businesses, our customers, and our reputation.

SEE SOMETHING. SAY SOMETHING.

Report suspicious emails, messages, or activity immediately.
Your awareness helps keep everyone safe.

Be Smart. Be Cautious. Be Secure. | Stay Informed. Stay Protected.