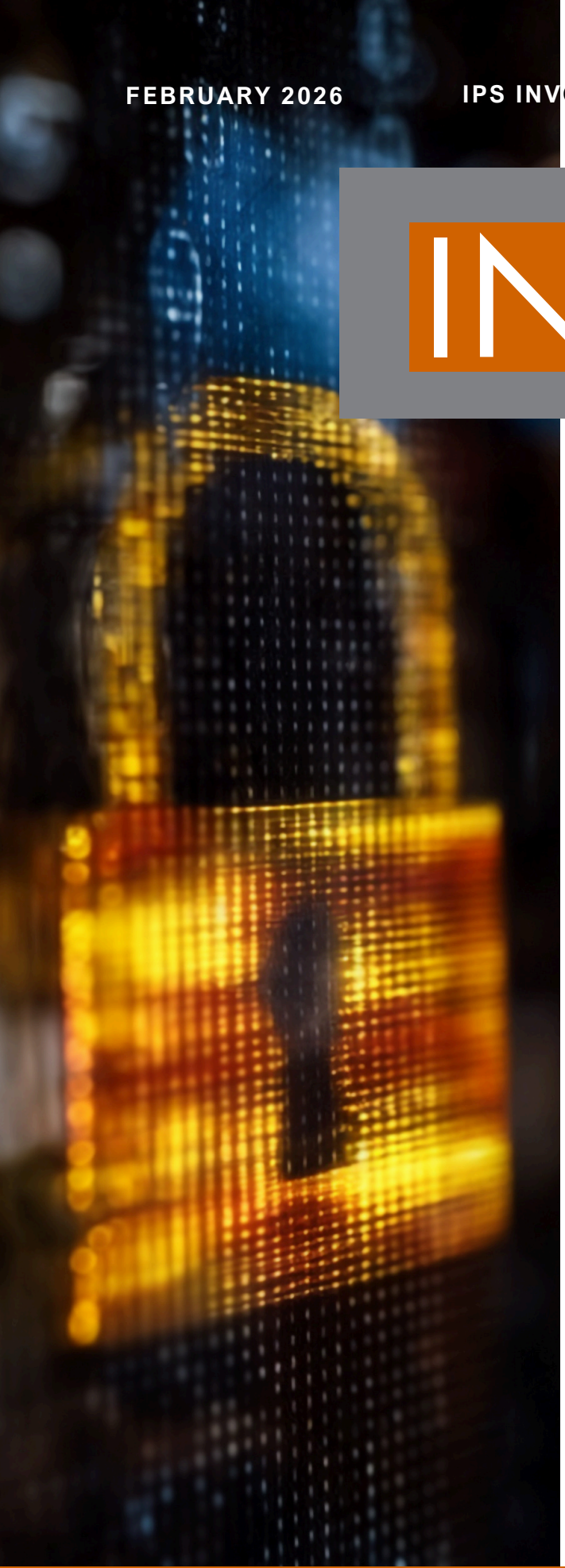
FEBRUARY 2026 IPS INVOICE PAYMENT SYSTEM ISSUE 177



INFOPAYS

PROTECTING YOUR BUSINESS FROM FRAUD AND CYBER RISK

As we continue 2026, security and fraud prevention remain top priorities for Canadian small businesses. With increasing reliance on digital tools, electronic payments, and remote access, safeguarding your company's financial and operational systems is essential.

At IPS, we see firsthand how evolving fraud tactics and cyber threats can impact cash flow, operations, and trust. This month, we want to share key insights to help you gain a stronger security posture.

DO - Best Practices That Reduce Risk

Access & Identity

- Use multi-factor authentication (MFA) on email, banking, accounting, and admin tools
- Apply least-privilege access - staff only get what they need, nothing more
- Review user access quarterly and immediately after employee exits

Email & Communication

- Train staff to spot phishing like urgent tones, payment changes, odd links
- Verify payment or banking changes verbally using a known phone number
- Use secure email gateways with spam, malware, and spoofing protection

Payments & Financial Controls

- Segregate duties - one person enters payments, another approves
- Set approval limits for wires, ACH/eTransfers, and refunds
- Enable transaction alerts for bank and payment platforms
- Reconcile bank accounts frequently (daily if possible)

IT & Systems

- Keep systems patched and updated (OS, browsers, firewalls, accounting software)
- Use endpoint protection (EDR/antivirus + firewall)
- Encrypt laptops, backups, and portable drives
- Back up data daily (offline + cloud, tested quarterly)

People & Process

- Run annual cyber & fraud training for all staff
- Have a written incident response plan like who does what and who to call
- Log and investigate anomalies, even small ones

DON'T - Common and Costly Mistakes

Access & Passwords

- Don't reuse passwords across systems
- Don't share logins or use generic accounts
- Don't keep ex-employees' access active

Email & Requests

- Don't act on urgent payment requests without verification
- Don't click links or open attachments from unknown or unexpected senders
- Don't trust emails just because they "look internal"

Financial Operations

- Don't allow one person full control over AR/AP, wires, and reconciliations
- Don't change vendor banking details based on email alone
- Don't ignore small discrepancies—they're often test fraud

IT Shortcuts

- Don't postpone security updates
- Don't rely on backups you've never tested
- Don't allow personal devices without security controls

PRO TIP

No money moves without a second human check.