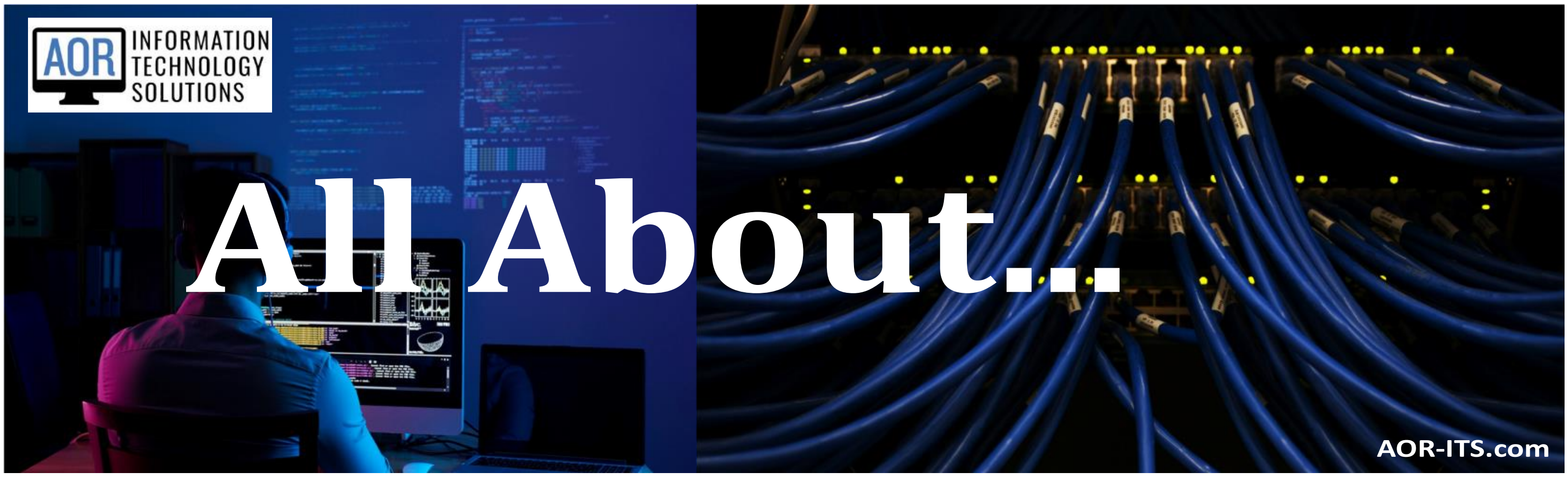

All About…

A Rising Threat Every Business Owner Needs To Take Seriously

Business e-mail compromise (BEC) is quickly becoming one of the most dangerous cyberthreats businesses face.

While these scams have challenged organizations for years, **the introduction of advanced AI tools has made them more sophisticated – and far more dangerous.**

In 2023, BEC scams caused $6.7 billion in global losses. Even more alarming, a study by Perception Point revealed a 42% increase in BEC incidents during the first half of 2024 compared to the same period the year prior. With cybercriminals harnessing AI to refine their techniques, this trend is only accelerating.

What Are Business E-mail Compromise (BEC) Attacks?

BEC scams aren't your average phishing attempts. They're highly targeted cyberattacks where criminals exploit e-mail accounts to trick employees, partners or clients into sharing sensitive information or transferring funds.

Unlike generic phishing, BEC scams often involve impersonating trusted individuals or organizations, making them far more convincing and effective.

Why Are BEC Attacks So Dangerous?

BEC scams are alarmingly successful because they rely on **manipulating human trust** rather than malware or attachments, which can often be detected by filters. Here's what makes them so destructive:

They can result in:

- **Severe Financial Losses:** One convincing e-mail can result in unauthorized payments or data theft. The average loss per attack exceeds $137,000, and recovering stolen funds is nearly impossible.
- **Operational Disruption:** An attack can grind business operations to a halt, leading to downtime, audits & internal chaos
- **Reputational Damage:** How do you explain to clients that their sensitive data may have been compromised?
- **Loss of Trust:** Employees may feel less secure, knowing their organization was vulnerable

Common BEC Scams To Watch Out For

BEC scams take many forms. Here are a few of the most common:

- **Fake Invoices:** Cybercriminals impersonate vendors and send realistic invoices requesting payment.
- **CEO Fraud**: Hackers pose as executives, pressuring employees to transfer funds under tight deadlines.
- **Compromised E-mail Accounts**: Legitimate accounts are hacked and used to send malicious requests.
- **Third-Party Vendor Impersonation**: Trusted vendors are spoofed, making fraudulent requests appear routine**.**

How To Protect Your Business From BEC

The good news? BEC scams are preventable with the right strategies in place:

1. **Train Your Team Like It's Game Day**
   - Teach employees to spot phishing e-mails, especially those marked "urgent"
   - Require verbal confirmation for any financial request
2. **Enforce Multifactor Authentication (MFA)**
   - MFA acts as a safety net, even if a password is compromised. Enable it on all accounts, particularly e-mail and financial platforms
3. **Test Your Backups**
   - Regularly restore data from backups to ensure they work, as a faulty backup during an attack could cripple your business
4. **Get Serious About E-mail Security**
   - Use advanced e-mail filters to block malicious links and attachments.
   - Audit access permissions regularly and revoke access for former employees immediately.
5. **Verify Financial Transactions**
   - Always confirm large payments or sensitive requests via a separate communication channel, like a phone call.

Next Steps For Security

Cybercriminals are evolving, but you can stay one step ahead. By training your team, securing your systems, and verifying transactions, you can turn your business into a fortress against BEC scams.

Want to ensure your business is protected? Start with a FREE Network Assessment to uncover vulnerabilities, secure your systems and keep cybercriminals out.

Let's stop BEC in its tracks – before it stops your business.

Click here or call our Glenside, PA office at 919-378-0969
to schedule a FREE Network (and Cybersecurity) Assessment today!