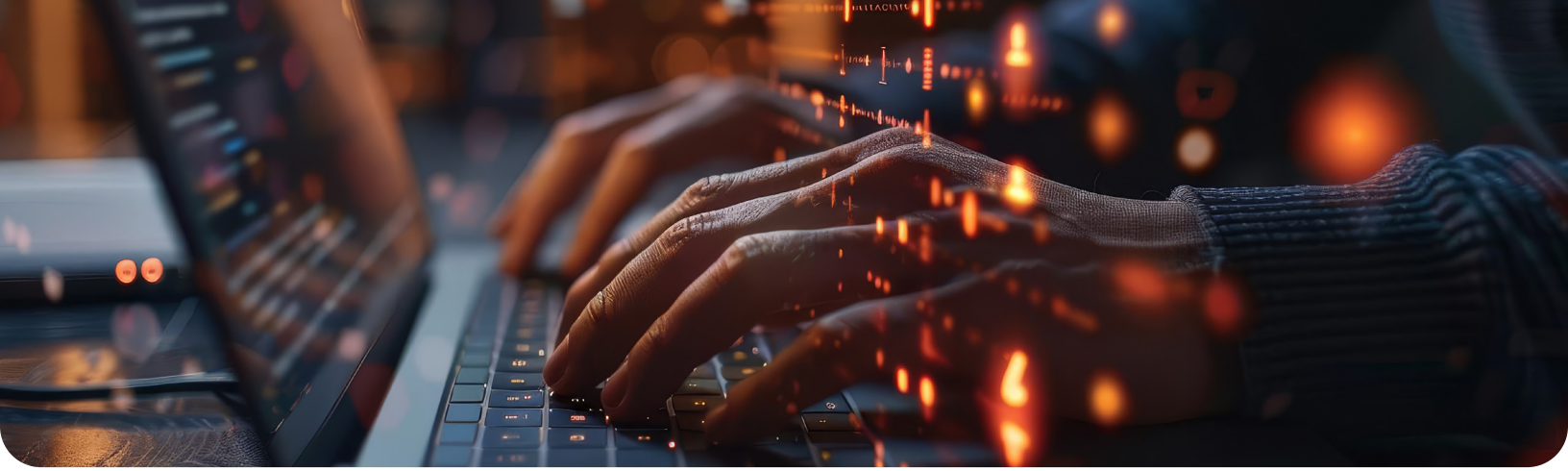


Don’t Fall for These Cyberthreats

A Comprehensive Guide

Cybercriminals are becoming more sophisticated, and businesses of all sizes are at risk. Whether it’s phishing emails designed to steal login credentials, ransomware attacks that lock you out of your data, or vulnerabilities in connected devices, cyberthreats have devastating consequences. Understanding these threats and taking proactive steps to protect your business can help avoid costly breaches, downtime and reputational damage. Here’s what you need to know.



1. AI-powered phishing attacks

Cybercriminals use artificial intelligence (AI) to craft highly convincing phishing emails, making spotting fraudulent messages more challenging than ever. These attacks trick employees into revealing sensitive information, such as passwords or financial details, or downloading malware onto your systems.

The risks

- Data breaches – Stolen credentials can lead to unauthorized access to sensitive business data.
- Financial loss – Phishing scams can result in fraudulent transactions, wire fraud or ransomware infections.
- Reputation damage – A data breach can erode customer and partner trust.

Did you know?

Phishing accounted for 83% of all email threats, while advanced attacks made up only 1%.

(Source: Acronis Cyberthreats Report, H2 2025)

How to protect your business

- Train your employees – Regularly educate your team on identifying phishing attempts, verifying email senders and reporting suspicious messages.
- Implement email security filters – Advanced filtering tools help detect and block phishing emails before they reach inboxes.
- Have an incident response plan – Be prepared with a clear strategy to respond to phishing attacks and mitigate damage quickly.
- Use multi-factor authentication (MFA) – Adding an extra security layer makes it harder for attackers to access accounts, even if passwords are compromised.



2.
Supply chain attacks

A supply chain attack happens when cybercriminals target a third-party vendor or supplier to gain access to your business. If one of your service providers is compromised, your data, operations and systems could be at risk.

The risks

- Data breaches – A compromised vendor could expose sensitive customer or business data.
- Operational disruption – Cyberattacks on suppliers can lead to downtime and business interruptions.
- Legal and financial impact – Businesses may face fines or legal action if customer data is compromised due to weak supply chain security.

Did you know?

Third-party vendor and supply chain compromise costs an average of $4.91 million.

(Source: IBM, July 2025)

Recommendations for your business

- Vet your vendors – Ensure third-party providers follow strict cybersecurity protocols before granting them access to your systems.
- Limit access – Only grant suppliers the minimum level of access they need to do their job and regularly review permissions.
- Include cybersecurity clauses in contracts – Hold vendors accountable for maintaining strong security standards.
- Conduct regular security audits – Assess your supply chain's security posture and address vulnerabilities.



3. Ransomware-as-a-Service (RaaS)

Ransomware attacks are on the rise, and cybercriminals are making it easier for anyone — even those with little technical expertise — to launch devastating attacks. This model, known as Ransomware-as-a-Service (RaaS), allows attackers to rent ransomware tools and profit from ransom payments.

The risks

- Data loss – Attackers encrypt your files and demand payment for their release.
- Operational downtime – Businesses can be forced to halt operations, leading to financial losses.
- No guarantee of recovery – Even if a ransom is paid, there's no guarantee that data will be restored.

Did you know?

80% of ransomware-as-a-service (RaaS) vendors advertise AI or automation features, operationalizing AI to scale existing attacks.
(Source: Acronis Cyberthreats Report, H2 2025)

How to protect your business

- Back up your data regularly – Store backups in secure, offsite locations and test recovery procedures.
- Educate employees – Train staff to recognize ransomware threats and avoid clicking on suspicious links or attachments.
- Keep software updated – Patch operating systems, applications, and plugins vulnerabilities.
- Use network segmentation – Restrict the spread of malware by separating critical systems from other network areas.



4.
Internet of Things (IoT) vulnerabilities

Connected devices, such as smart cameras, thermostats and industrial sensors, improve efficiency but also introduce security risks. Many IoT devices have weak security settings, making them easy targets for hackers.

The risks

- Data breaches – Hackers can exploit IoT vulnerabilities to access your systems.
- Network compromise – Compromised devices can be used to launch larger-scale cyberattacks.
- Physical security risks – Attackers can manipulate smart locks or security systems.

Did you know?

24% of organizations say their greatest challenge to becoming cyber resilient is a lack of visibility across IT, OT and IoT environments.

(Source: World Economic Forum, January 2026)

Recommendations for your business

- Segment your network – Keep IoT devices on a separate network from critical business systems.
- Update device firmware – Regularly install security patches and updates.
- Monitor activity – Set up alerts for unusual behavior on connected devices.
- Use strong passwords – Change default credentials and use unique, complex passwords for each device.

5.
Insider threats

Not all cyberthreats come from external hackers — some originate from within an organization. Whether it's a disgruntled employee seeking revenge or one who accidentally clicks on a phishing link, insider threats are just as dangerous as external attacks.

The risks

- Data leaks – Sensitive business information can be exposed or stolen.
- System compromise – Employees with access to critical systems can cause intentional or unintentional damage.
- Reputation damage – A security breach caused by an insider can harm your company's trust and credibility.

Did you know?

$4.29 million is the average cost of malicious insider attacks.

(Source: IBM, July 2025)

How to protect your business

- Provide regular security training – Educate employees on cybersecurity best practices.
- Limit access to sensitive data – Only grant access on a need-to-know basis.
- Monitor internal activity – Use security tools to detect unusual behavior.



Protect your business from cyberthreats

Cybersecurity is a growing challenge, but you don't have to navigate it alone. Our experts help assess risks, implement strong defenses and protect your business against evolving threats. Contact us today to discuss how we can help secure your business:

Devopsx Company Limited
Email: tung@devopsx.vn
Phone: +84582686866