What To Do Before You Get Hacked

Here's what we know: The number of cyber threats are at an all-time high. Many organizations assume they are protected from cyber threats, but the reality is they are not. Here are five things you can do to stay protected.

1 Incident Response Plan

Work with a dedicated team like PCA to identify:

- What is considered an incident
- Different levels of incidents
- Incident response procedures
- What happens post-incident

2 Disaster Recovery Plan

This will address larger questions about how your business can resume normalcy after a disaster disrupts your operations. You may also consider cyber insurance.

3 Data Security & Risk Assessment

Understanding your unique IT risk and identifying your most protected assets will be a major benefit. It exposes any potential IT weaknesses and provides time to resolve!

4 Employee Education

90% of breaches involve human error, which is why you need ongoing cybersecurity training for your team. Hackers continue to become more sophisticated!

5 Solutions & Tools

There are a variety of solutions and tools you can implement to protect your assets, including:

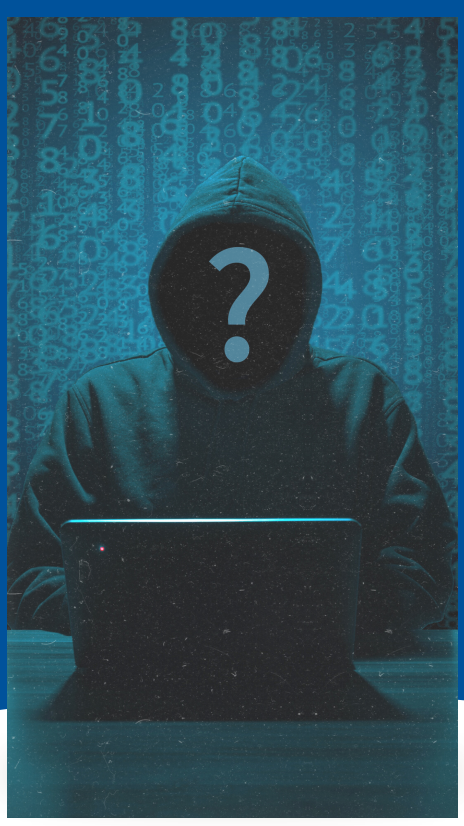
- Firewall solutions
- Multi-Factor Authentication (MFA)
- Server and endpoint security/monitoring
- And more! Browse our cybersecurity portfolio!

Interested in working with a Managed Service Provider for your core cybersecurity needs? Contact the PCA team today!

www.pcatg.com | 716.632.5881 | info@pcatg.com

What To Do After You Get Hacked

With cybercrimes affecting many businesses across all industries, it's imperative to have a plan in place in the event an incident occurs. What should you do if you get hacked?



1 Be Aware & Notify Your CISO

You'll want to activate your Incident Response Plan:

- What triggered the incident?
- Analyze all existing tools and solutions
- Verbally communicate to the appropriate contacts to prevent any additional losses.

2 Categorize The Incident

- **Green:** Originates from and impacts non-production company systems and is mitigated.
- **Yellow:** Originates from/impacts company's production systems and cannot be prevented.
- **Red:** Production assets are at immediate risk; potential to spread to other systems; a breach!

3 Protect The Evidence

Although evidence is not collected at this step, it's crucial to preserve the integrity of any potential evidence. If deliberate destruction is considered likely (by a suspect or attacker), more aggressive actions may be required.

4 Communication & Recovery

This step will vary based on the incident level (green, yellow, or red). All levels should involve notifying the appropriate contact, determining which systems were affected, documenting incident response, and recovery.

5 Incident Follow Up

During yellow and red level incidents, we suggest several key follow ups: Determining root causes, analyzing the strength of the existing controls that defend against attacks, and reviewing any lessons learned. If appropriate, file any documents with the FBI/U.S. Secret Service and re-analyze your plan!

Interested in working with a Managed Service Provider for your core cybersecurity needs? Contact the PCA team today!

www.pcatg.com | 716.632.5881 | info@pcatg.com