Cyber-Security SAFETY REPORT

A recent survey of 1,300 U.S. employees conducted by Horizon Dataworks exposes a critical gap between cybersecurity awareness and daily employee behavior, putting organizations at serious risk of data loss. Below are the top five takeaways every business should know.

1. Human Error: The Leading Cause of Security Breaches

A staggering **95% of all security incidents** stem from simple human errors.

Poor quality assurance practices are costing companies nearly **$200 billion** annually.

2. Delayed Updates Create Long-Term Security Gaps

Over **40%** of employees admitted to delaying critical updates for six months or longer to prioritize other work.

64% of security breaches exploit known vulnerabilities that remain unpatched.

3. Politeness Over Protection: A Dangerous Trade-Off

1 in 4 workers still share sensitive company passwords via text or email.

52% would let colleagues use their computers, risking sensitive data exposure.

4. Risky Clicks: Employees Play with Fire

51% have clicked on links in emails or messages they didn't recognize.

57% have installed unauthorized browser extensions on work devices, opening backdoors to hackers.

5. Data Loss is More Common Than You Think

4 out of 5 respondents have accidentally deleted important files.

25% of employees have lost data within cloud platforms like G Suite or Microsoft Office 365.

PROTECTED HARBOR
Your Trusted Partner in Cybersecurity

Call us: +1 201-957-1616
Visit: protectedharbor.com
Email: sales@protectedharbor.com

Don't let your organization be part of these statistics—reach out today to safeguard your business!