GRC³

How to Combat Security Risks While Working From Home

The pandemic accelerated work-from-home adoption virtually overnight. While many organizations embraced hybrid models, this rapid transition exposed critical security vulnerabilities that employees and companies weren't prepared to handle.

Schedule a Demo

The Security Challenge

15%

Security Awareness

Only 15% of people know how to protect themselves from cyberattacks

Taking work computers home creates serious risks: data loss, data theft, and lack of built-in security measures. The key questions: Who has access to your home office? How safe is your network? Can someone steal your laptop?

The good news: You can avoid these risks by being responsible and alert.

3 Most Common Security Challenges

Unsecured WiFi Networks

Home networks lack company security measures like antivirus programs and firewalls, making them easier targets for malware and malicious attacks.

Phishing Scams

Hackers steal personal information through fraudulent emails, SMS, or calls. Coronavirus-themed phishing attacks are on the rise, targeting passwords and bank details.

Using Personal Devices

Personal laptops often lack appropriate security measures and backup mechanisms, directly exposing data to unsecured environments and increasing malware risk.

GRC³

Spotting Phishing Scams

01

Check sender's email address

Verify the email comes from a legitimate source

02

Examine the URL carefully

Look for slight variations like www.1bank.com vs www.bank.com

03

Look for poor grammar

Professional companies rarely send emails with errors

04

Never open attachments

Suspicious attachments can contain malware

05

Don't reply to suspicious emails

Forward to the legitimate company instead

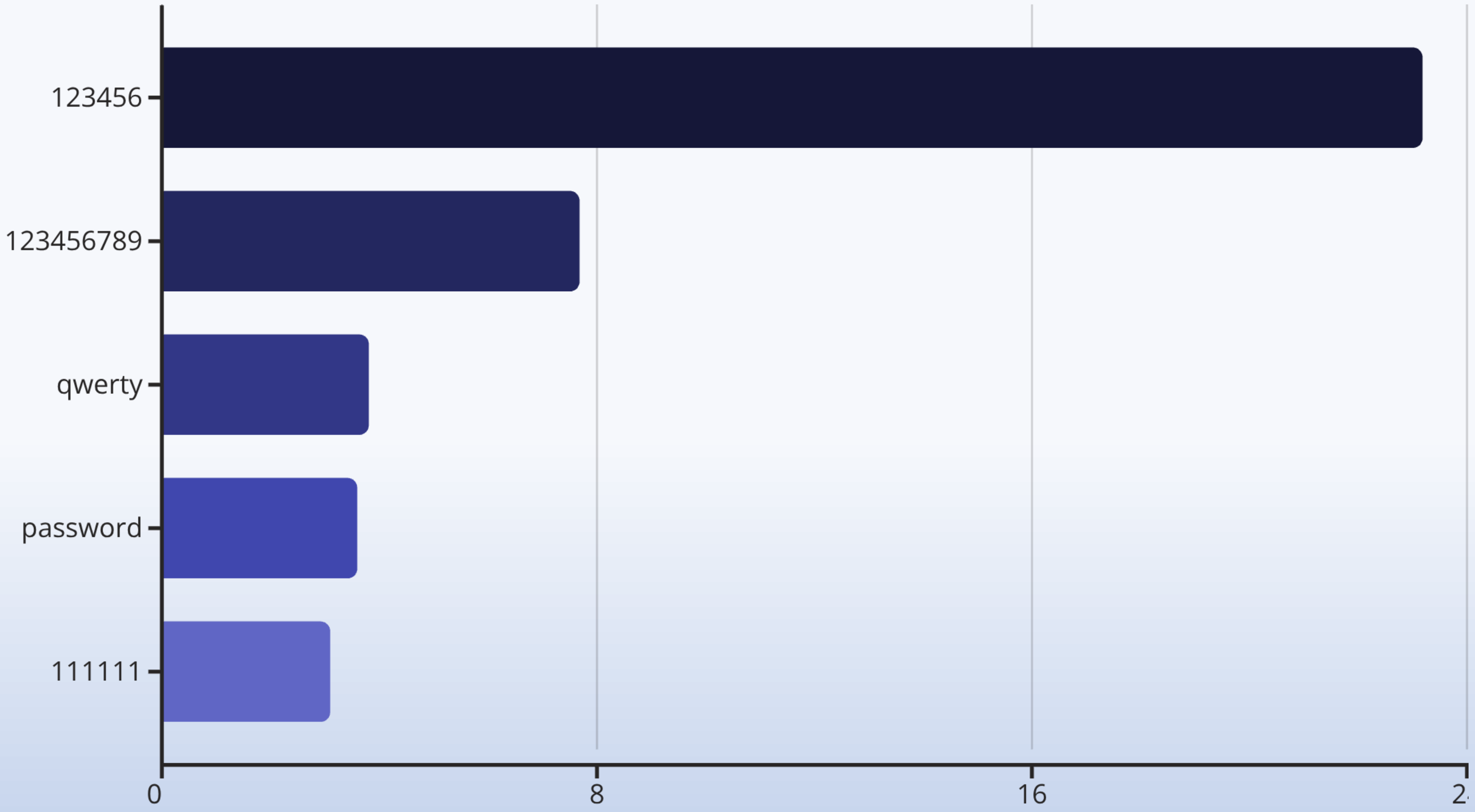
06

Alert your co-workers

Share information to protect the entire team

The Password Problem

Most Common Passwords in 2019



Password Best Practices

- Create strong passwords with symbols and numbers
- Change passwords every 30-90 days
- Use password managers like KeePass
- Never write passwords on post-its

GRC³

Essential Device Security

1

Use Company Computers Only

Personal computers lack proper safeguards and can infect secure networks with malware. Using work computers for personal tasks also creates privacy risks.

2

Lock Your Devices

Always lock your screen when leaving your workstation. Protect business phones with strong passwords, not pattern locks which are vulnerable to social engineering.

3

Never Leave Devices Unattended

Physical access is a real threat. Unattended devices can be stolen or accessed, allowing unauthorized data downloads or deletion.

Partner With GRC³ for DPDP Success

www.grc3.io (GRC Cube)

Contact:

Nidhi P. - Nidhi.p@grc3.io / +91 9004735605

Mayuri B. - mayuri.b@grc3.io / +91 8097235523

Pooja D. - pooja.d@securetain.com

Charu P. - charu.pel@grc3.io

Network Security Essentials

Avoid Unsecured WiFi

Encrypted WiFi protects data from interception. Unsecured networks expose login information, emails, and instant messages to third parties.

Use VPN

Virtual Private Networks mask your IP address and create encrypted connections, providing greater privacy than even secured WiFi hotspots.

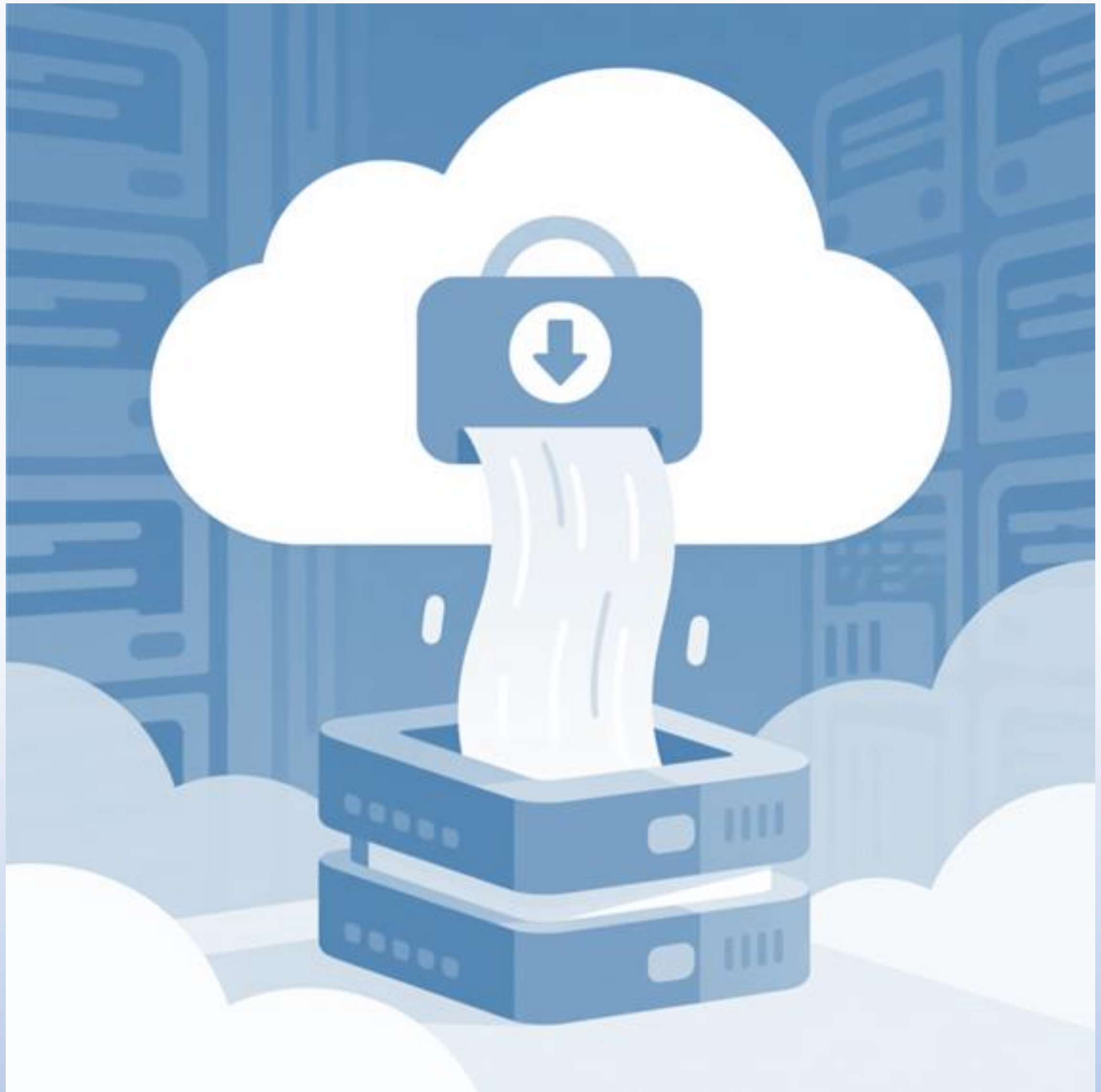
Enable Firewalls

Firewalls monitor traffic and block malicious programs. Turn on built-in firewalls on your device and router as your first line of defense.

Defense Systems

Antivirus Programs

Data Backup



GRC³

Education is Key

Human error is the most common security risk

Attend Security Training

Participate in periodic cybersecurity education conducted by your company's security officer.

Ask Questions

Contact your IT department or security expert for guidelines on remote work responsibilities.

Share Information

Report suspicious activity and alert co-workers about potential threats immediately.

Why GRC^3.io - The Fix: One Unified, AI-powered GRC Platform

Lower Total Operating Cost, Lower Risk, Continuous Trust. GRC^3 is LIVE!

One Platform — Five Integrated, AI-Enabled and Proven to Scale.

5 Integrated Products	GRC3 Unique Feature	+ AI Advantage
Compliance / Frameworks	Unified engine supporting 350+ global frameworks. Offers real-time auto-mapping and change tracking.	Maps controls, builds smart workflows, and generates live policies.
Data Privacy	Pre-configured for 100+ global privacy laws. Provides centralized consent and rights management.	Accelerates compliance, consent tracking, and reporting.
Third Party Risk (TPRM)	Real-time vendor risk visibility with automated assessments and prioritization.	Closes gaps faster, auto-prioritizes risk, improves collaboration.
+ IT Operations	Cross-module linkage between breach, response, and control management	Connects incidents to controls, triages tasks, and forecasts risk.
Internal Audit	End-to-end audit automation and prioritization that shortens cycles.	Automates evidence, optimizes scope, maintains continuous audit readiness.

GRC³

Organizations Must Take Action

Companies with remote employees must ensure the same security conditions as in-office workers. This requires comprehensive policies and support.

Create Remote Working Policies

Develop clear guidelines that help employees navigate security incidents and adapt to remote work challenges.

Implement Technical Measures

Explain password creation, device protection, network login procedures, and incident response protocols.

Provide Organizational Support

Ensure employees have VPN access, security tools, and ongoing education to maintain data protection standards.

GRC^3

Benefits of GRC^3 Platform

Accelerate Compliance
Build Trust
Scale with Confidence

Get Your Free Maturity Assessment

Assess Compliance Maturity ▽

Assess Privacy Maturity ▽

As risk and regulatory demands surge, businesses need more than spreadsheets. GRC3 is a platform designed and developed by practitioners to **eliminate silos** between compliance, cybersecurity, internal audit, privacy, and vendor risk - enabling enterprises to **scale securely, accelerate revenue, and prove trust** enterprise-wide.

Learn More →