



CYBERSECURITY TIPS

31 practical reminders to strengthen everyday cyber resilience

People
Prevention
Preparedness
A Stronger Tomorrow

TIP #1

Cybersecurity is not just defense. Done right, it can reduce disruption, improve efficiency, and save money.



TIP #2

Don't think "it won't happen to me." Every business faces cyber risk.



TIP #3

SMBs are the biggest target for cyberattacks. Access adds up.

Review permissions regularly and remove what people no longer need.



TIP #4

Business size or industry doesn't matter - if you have data, you are at risk.



TIP #5

Hackers love SMBs because they have valuable data and they're relatively unprotected and unmonitored.



TIP #6

You can often hear: "There are only two types of organizations today - those that have been hacked and those that have been hacked but just don't know it yet."



TIP #7

Security is only as strong as the weakest link, and sometimes that weak link is beyond your four walls.



TIP #8

Most cyber incidents are due to insider threats (your employees). Cybersecurity education for your employees is key!



TIP #9

Policies and training will not automatically fix all security issues.



TIP #10

Cybersecurity is NOT just an IT issue - all employees, even third parties you do business with, play a role in keeping your company safe.



TIP #11

Realize that even your staff's personal devices (including wearables) can compromise a network.



TIP #12

Security is not set it and forget it. Threats change, and your defenses need to keep up.



TIP #13

There is no silver bullet in cybersecurity. Strong protection comes from layers.



TIP #14

Don't overlook physical security. A lost device can be just as damaging as a digital attack.



TIP #15

Don't assume you'll know when something is wrong. Some threats are built to stay hidden.



TIP #16

If a breach happens, know who needs to be told and when.



TIP #17

Cybersecurity takes ongoing attention. Review, test, and update your defenses regularly.



TIP #18

A layered approach is stronger. Protect identities, users, endpoints, networks, cloud apps, and data.

Protect the network (FW), protect the systems (patching and next-gen anti-virus), email (still #1 entry point), and protect against data loss (backup)



TIP #19

Endpoints are a common target. Protect every device that connects to your business.



TIP #20

Antivirus and firewalls matter, but they are not enough on their own.



TIP #21

Avoiding suspicious emails helps, but threats can come from trusted accounts, websites, apps, and stolen credentials too.



TIP #22

A password alone does not make an account safe.



TIP #23

Use strong, unique passwords, a password manager, and MFA whenever possible.



TIP #24

Be careful on public WiFi, especially when accessing sensitive information. Use secure connections and strong access controls.



TIP #25

Disconnecting devices doesn't eliminate the risk.



TIP #26

When it comes to hackers, think highly organized hacking organizations, not a teen in a hoodie working in the basement.



TIP #27

Being good at IT does not automatically make someone a cybersecurity expert.



TIP #28

Cybersecurity expertise is hard to build and keep in house.



TIP #29

Working with a Managed Service Provider (MSP) like TPx is often more cost-effective than maintaining an infrastructure with in-house staff alone.



TIP #30

Managed services can reduce the burden on your team and help avoid the costs tied to downtime, hiring, and turnover.



TIP #31

The cost of prevention is usually easier to manage than the cost of recovering from a major incident.



Smarter
Security
Stronger
Business

