



Cyber Security Tips

Cybersecurity tip #1

TPX

Cybersecurity is not just a form of defense – it is also a strategic advantage as it can boost efficiency and save money.

Cybersecurity tip #2

TPX

Don't think "it won't happen to me". The odds are it will.

More than half (55%) of smaller businesses reported at least one data breach in the previous year – Ponemon Institute's 2017 Study

Cybersecurity tip #3

TPX

SMBs are the biggest target for cyberattacks:

According to 2017 Ponemon study, more than 61% of SMBs have been breached in 2017

Cybersecurity tip #4

TPX

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

Cybersecurity tip #5

TPX

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

Cybersecurity tip #6

TPX

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."

You've been hacked

I know

What! I didn't know!

Cybersecurity tip #7

TPX

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

SECURITY

Cybersecurity tip #8

TPX

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

Cybersecurity tip #9

TPX

Policies and training will not automatically fix all security issues.

Zzz

Cybersecurity tip #10

TPX

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

Accounting

CONFIDENTIAL

HR

Vendor

SAFE

Cybersecurity tip #11

TPX

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

Cybersecurity tip #12

TPX

Security is not a set-it and forget-it type of thing. Keeping a business cybersafe is a continuous effort.

Cybersecurity tip #13

TPX

There's no silver bullet to security, but you can drastically minimize your chances of being a victim of a cyberattack by practicing good "cyber hygiene".

Cybersecurity tip #14

TPX

Physical security (devices, paper records, hard drives) shouldn't be treated separately from digital security.

Cybersecurity tip #15

TPX

Don't think that you will know if your systems are infected. Now there are programs that are nearly undetectable.

Cybersecurity tip #16

TPX

Breach reporting isn't optional: If you are hit by ransomware, don't try to cover it up.

Cybersecurity tip #17

TPX

To keep your company cybersafe, you need to continuously monitor your systems, conduct internal audits, and review, test, and evaluate contingency plans.

Cybersecurity tip #18

TPX

A layered approach is the most effective.

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

Cybersecurity tip #19

TPX

The endpoint is often the most vulnerable point, thus represents the greatest risk of loss or compromise of data, and needs protection.

Cybersecurity tip #20

TPX

Having an anti-virus and a firewall is important but not enough.

Cybersecurity tip #21

TPX

Even if you don't open emails from people you don't know— you're still vulnerable to malware!

Cybersecurity tip #22

TPX

Don't assume that whatever is protected by a password is safe.

Cybersecurity tip #23

TPX

Passwords are surprisingly easy to hack – ALWAYS use a password manager.

PASSWORD VAULT

Cybersecurity tip #24

TPX

Don't ever use public WiFi to access sensitive information, like banking, online shopping, even email and social media. When in doubt, use a Virtual Private Network (VPN).

Cybersecurity tip #25

TPX

Disconnecting devices doesn't eliminate the risk.

Cybersecurity tip #26

TPX

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

HACKERS HQ

Cybersecurity tip #27

TPX

Realize that technical expertise in IT and cybersecurity are not the same.

Cybersecurity tip #28

TPX

Finding cybersecurity experts isn't easy (or cheap): Unemployment in the cybersecurity field has dropped to a stunning 0% and there are 1 million unfilled jobs.

Cybersecurity Ventures research

Cybersecurity tip #29

TPX

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

In-house team

TPx

Cybersecurity tip #30

TPX

With MSP, you're cutting costs of downtime and business interruption, spending less for salaries, hiring and turnover.

Cybersecurity tip #31

TPX

While the costs tied to protection can be daunting, especially for small organizations, the costs only increase after an attack. It is cheaper to pay for prevention than for rebuilding infected systems and replacing lost information.

ATM

OUT OF FUNDS