TOP 10 SECURITY BEST PRACTICES FOR SMBS

01 COMMON PASSWORDS ARE BAD PASSWORDS
Passwords are your first line of security defense. Cybercriminals attempting to infiltrate your network will start by trying the most common passwords.

*BEST PRACTICE:* Create a list of long, strong, unique passwords. Include numbers, upper case, lower case, and non-alphabetic characters.

02 SECURE EVERY ENTRANCE
A cybercriminal can enter your network through the front door. By locking down your network, you increase your security.

*BEST PRACTICE:* Consider all the ways someone could enter your network, then ensure that only authorized users can do so.

03 SEGMENT YOUR NETWORK
A way to protect your network is to separate your network into zones and protect the zones appropriately. One zone may be for critical work only, while another may be a guest zone where customers can surf the internet, but not access your work network.

04 DEFINE, EDUCATE, AND ENFORCE POLICY
Actually HAVE a security policy (many small businesses don’t) and use your Threat Prevention device to its full capacity. Spend some time thinking about what applications you want to allow in your network and what apps you do NOT want to run in your network.

Educate your employees on acceptable use of the company network. Make it official. Then enforce it where you can. Monitor for policy violations and excessive bandwidth use.

05 BE SOCIALLY AWARE
Social media sites are a goldmine for cybercriminals looking to gain information on people, improving their success rate for attacks. Attacks such as phishing, spearphishing, or social engineering all start with collecting personal data on individuals.

06 ENCRYPT EVERYTHING
One data breach could be devastating to your company or your reputation. Protect your data by encrypting sensitive data and making it easy for your employees to do so.

Ensure encryption is part of your corporate policy.

07 MOUNT YOUR NETWORK LIKE YOUR CAR
Your network, and all its connected components, should run like a well-oiled machine. Regular maintenance will ensure it continues to roll along at peak performance, hitting less speed bumps along the way.

08 CLOUD CAUTION
Cloud storage and applications are all the rage, but be cautious. Any content that is moved to the cloud is no longer in your control. Cybercriminals are taking advantage of weaker security of some cloud providers.

09 DON’T LET EVERYONE ADMINISTRATE
Laptops can be accessed via user accounts or administrative accounts. Administrative access allows users much more freedom and power on their laptops, but that power can move to the cybercriminal if the administrative account is hacked.

*BEST PRACTICE:* Keep administrative access to your network limited to key individuals only.

10 ADDRESS THE BYOD ELEPHANT IN THE ROOM
BYOD (Bring Your Own Device) is a trend that continues to push forward. Don’t avoid the elephant in the room! It all comes back to educating the user.

SECURITY BEST PRACTICES FOR SMBS

1. COMMON PASSWORDS ARE BAD PASSWORDS
2. SECURE EVERY ENTRANCE
3. SEGMENT YOUR NETWORK
4. DEFINE, EDUCATE, AND ENFORCE POLICY
5. BE SOCIALLY AWARE
6. ENCRYPT EVERYTHING
7. MOUNT YOUR NETWORK LIKE YOUR CAR
8. CLOUD CAUTION
9. DON’T LET EVERYONE ADMINISTRATE
10. ADDRESS THE BYOD ELEPHANT IN THE ROOM