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: Ensure use of long (over 8 characters) and complex passwords (include lower case, upper case, numbers, and non-alpha characters).

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, where another may be a guest zone where customers can surf the internet, but not access your work network.

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 moves to the cybercriminal if the administrator account is hacked.

SECURE EVERY ENTRANCE

All it takes is one open door to allow a cybercriminal to enter your network. Just like you secure your home by locking the front door, the back door and all the windows, think about protecting your network in the same way.

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.

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, spearphish, or social engineering all start with collecting personal data on individuals.

ENCRYPT EVERYTHING

One data breach could be devastating to your company or your reputation. Protect your data by encrypting sensitive data and make it easy for your employees to do so. Ensure encryption is part of your corporate policy.

MAINTAIN 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 perform at its best, hitting less speed bumps along the way.

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. And cybercriminals are taking advantage of weaker security of some cloud providers.

ADDRESS THE BYOD ELEPHANT IN THE ROOM

Start with creating a Bring-Your-Own-Device policy. BYOD is here to stay, but a model that combines a good security risk management strategy with a solid education program can be both effective and beneficial.

TOP 10 SECURITY BEST PRACTICES FOR SMBs

- COMMON PASSWORDS ARE BAD PASSWORDS
- SECURE EVERY ENTRANCE
- DEFINE, EDUCATE, AND ENFORCE POLICY
- BE SOCIALLY AWARE
- ENCRYPT EVERYTHING
- MAINTAIN YOUR NETWORK LIKE YOUR CAR
- CLOUD CAUTION
- ADDRESS THE BYOD ELEPHANT IN THE ROOM
- DON'T LET EVERYONE ADMINISTRATE
- SEGMENT YOUR NETWORK

Let's talk about the best practices that you can take to protect your business. Start by securing your home office from the inside out. Then, consider implementing a threat prevention device to help protect your network from external threats. By following these best practices, you can significantly reduce the risk of a successful cyberattack.

Check Point Software Technologies Ltd. All rights reserved.