CYBER SECURITY TIP GUIDE

COMCAST BUSINESS
AUTHORIZED CONNECTOR

Cyberattacks occur daily. More than half (**55 percent**) of SMBs and Mid-Market companies with fewer than 1,000 employees have experienced a cyberattack, while **43 percent** of all attacks target small businesses.

Hackers seek companies that carry information with a dollar value – medical records, credit card information, Social Security numbers, bank account credentials or proprietary business information.

To protect your business, you need to understand the different threats it faces.

KNOW THE THREATS

To break into your company, a hacker is going to most likely using one of these methods:

Ransomware
Malware that locks computers and encrypts the data, preventing businesses access, often until a ransom is paid.

Phishing
Entices users to click an email or attachment containing a virus that then infects their computer, and possibly other machines.

Malvertising
Short for "malware advertising," it consists of delivering malware to a network after a user clicks on an apparently legitimate ad.

Clickjacking
Hiding hyperlinks to compromised web pages in website links where users reveal personal data – which is then stolen.

Drive-By-Downloads
A dirty trick that downloads malware into networks. Sometimes from a pop-up window or even a compromised website.

DON'T BE A VICTIM – FOLLOW THESE 10 BEST PRACTICES

1 Set a Strategy Understand the threats and what cybercriminals are after in order to build up your defenses.	**6 Implement Patch Management** Have a strict patching policy so users don't ignore software update prompts.
2 Educate Users Train employees to turn them into the front line of defense. Uninformed workers can lead to risk.	**7 Maintain a Firewall** Use a firewall to create a barrier that determines which content to allow into your network and which to block.
3 Apply Advanced Tools Acquire tools that deliver endpoint protection, secure the network through firewalls, and perform threat analysis.	**8 Don't Forget Mobile** Include mobile devices into security strategies as computing is becoming more mobile.
4 Invest in Expertise Work with experts who have a full grasp of cybersecurity. A managed security services provider (MSSP) is a great option.	**9 Strengthen Password Management** Change passwords regularly and be sure to use combinations that are harder to crack than commonly used words.
5 Deploy Endpoint Security Select platforms with advanced protection, including machine learning technology that can identify suspicious code as malware, block it and start remediation.	**10 Implement Backup and Recovery** Failure to backup data exposes a company to disaster because if you suffer a data loss, that data is gone forever. It also puts companies in a very weak position if struck by ransomware.

IF ALL ELSE FAILS, PREPARE FOR A BREACH WITH AN INCIDENT RESPONSE PLAN (IRP)

Most businesses – **about 75%** – lack an incident response plan (IRP), which outlines what steps to take and who is responsible for what actions following a security breach. IRPs should include these fundamental components:

- **Build a Cross-Functional Team** – Members should include representatives from various departments.
- **Clarify Response Roles** – Employees need to know what steps to take after a breach.
- **Define Security Incidents** – Outline different incidents and prioritize the most important.
- **Anticipate Hackers' Moves** – Immediately check the systems that house the most critical data to determine if they've been breached.
- **Specify Procedures** – Following an incident, detail the prescribed recovery steps.
- **Document and Communicate** – Document every action, process and procedure and then share with the team.
- **Test the Plan** – Periodically assess the plan to ensure it is effective, it'll save you time and damage.

If your business doesn't have an IRP, start working on one today to minimize the damage in the event of a breach.

TO LEARN MORE ON CYBERSECURITY VISIT:

The Comcast Business Community

COMCAST BUSINESS
AUTHORIZED CONNECTOR