COMCAST
BUSINESS

SMALL BUSINESS GUIDE

The Small Business Guide to Cybersecurity

Small businesses don’t have big business cybersecurity resources, but they still face the same threats. Fortunately, through education, technology, and best practices, small businesses have the tools at their disposal to help protect their businesses, employees, and customers from an ever-changing array of cybersecurity threats.

In this practical guide, we’ll explore user education, threat monitoring and mitigation, device management and incident responses, with clear takeaways to help you improve security across your business.

User education

When hackers succeed, it's often because they targeted unsuspecting end users. Well over half of the breaches that happen in the US, in fact, involve company insiders—either intentionally or accidentally. Keeping employees trained on current threats is one of your strongest lines of defense against cybersecurity risks.

34%

of security incidents were caused by non-malicious user error.

SOURCE: Foundry

Conduct training on a regular basis. Threats evolve over time, so make it a regular practice to formally train employees on online hygiene. If you don't have anyone on staff, consider bringing in an outside trainer.

Show employees what's in it for them. Good online hygiene doesn't just protect company information—it protects their personal information, too.

Start training during onboarding. Make new hires aware of your security policies and best practices from the outset.

Share updates in real time. Keep your team in the loop about new threats and encourage employees to report threats or attacks.

Key Tips for Employees

Beware of suspicious emails

Don't click suspicious links

Verify purchases

Be careful about the information you share on social media

Threat monitoring, firewalls, and anti-virus

When it comes to security tools, the best defense is a good mix. Threat monitoring, firewalls, and anti-virus solutions are all valuable cybersecurity measures, but none of them are silver bullets—they should be used in tandem with each other and alongside smart online hygiene practices

Here are the key elements.

Threat monitoring and mitigation. Threat monitoring tools actively intervene to block malicious threats like malware, ransomware, phishing, and botnet infections. They also block employees and guests from accessing compromised websites and infected links. It's important to select tools that frequently update to help protect against the newest threats, and cover every connected device on your network.

Anti-virus. Anti-virus tools detect and block malicious files, but many only block malware they recognize based on signatures that have been written into the AV software.

Firewalls. Firewalls allow only authorized traffic or content using configured controls, like access denial to IP addresses known to deliver malware. Even if a malicious payload is delivered, firewalls can prevent it from communicating with control-and-command servers.

Password and device management

Think about all of the connected devices on your business network. From company devices to employees' personal phones to guest devices, each of them represents a potentially vulnerable endpoint, and each contains myriad pathways into your network through apps and systems. One weak password, bad password management, or a few errant keystrokes on a suspicious website can invite a breach.

Here are key tips.

Patch management. Software and system updates often close previous security loopholes. Not updating in a timely fashion can open you up to threats, as hackers become aware of loopholes and try to exploit them. Enact strong patch management policies or, even better, automate software updates.

Encrypt data where appropriate. All businesses should encrypt any personally identifiable information they collect, as well as any other potentially sensitive information, like company financials or intellectual property.

Leverage a password management solution. Strong passwords are essential, but documenting and remembering them can be a challenge. Password management tools not only generate strong passwords, but also store them for easy access.

Be careful with external devices like flash drives. Flash drives and other external devices can carry malware that's loaded onto your device when connected—some even coming from disreputable sources preloaded with malicious programs. If they're used with multiple devices on your network, infections can spread quickly.

Don't neglect physical security. Lock your device when you aren't using it and ensure storage areas, server rooms, and other locations with sensitive information or devices are secured.

Enact strong policies and practices

Embed a proactive security stance into your company's DNA. By codifying certain elements of your cybersecurity approach through policy and process, you can ensure that cybersecurity remains an ongoing priority.

Patch management. Threat monitoring tools actively intervene to block malicious threats like malware, ransomware, phishing, and botnet infections. They also block employees and guests from accessing compromised websites and infected links. It's important to select tools that frequently update to help protect against the newest threats and cover every connected device on your network.

Encrypt data where appropriate. All businesses should encrypt any personally identifiable information they collect, as well as any other potentially sensitive information, like company financials or intellectual property.

Backup your data. It's a best practice, but can also help with recovery in the event of a breach or ransomware attack.

Use VPNs when accessing sensitive applications remotely. Especially in a remote work setting, virtual private networks allow employees to access company networks and systems through a secure connection.

Operate in a zero-trust environment Zero-trust is a security model built around the idea that no device or user, either inside or outside an organization, should be trusted inherently. All access is cut off until identities are verified, dismantling the traditional inside-outside view of security: that anything inside the company's perimeter was safe, and anything outside wasn't.

Incident response planning

Strong defense capabilities are essential, but no defense is ironclad. It's essential to not only mount defenses, but also to prepare a detailed plan outlining what to do if you do find yourself the victim of a cyber attack.

Team designation. Designate cross-functional team members who should respond in the event of a breach, or have a cybersecurity consultant or contractor easily accessible to assist.

Clarify roles. For an in-house response team, ensure each member knows their roles and responsibilities in the event of a breach. Jobs would include identifying and isolating affected systems and devices, diagnosing how far an infection has spread, and more. Ensure that team members have the access and authority they need to carry out their responsibilities.

Define what you consider a security incident. Does an attempted, but unsuccessful, hack count as an attack? Determine the parameters that warrant a coordinated response for your organization.

Specify procedures. Your plan should be detailed and clear in its prescribed steps for recovery. Include contingencies such as having to resume operations from an alternative location and how to respond if the breach occurs after hours or when response team members are away.

Every day in business is a big day. To help stay ready for what's next, whether that might be costly malware, ransomware, bots, or a phishing attempt, small businesses need to implement cybersecurity measures that include anti-virus programs, firewalls, and network security solutions that proactively help protect all devices connected to your network. See how Comcast Business SecurityEdge™ can help protect the Internet-connected devices that employees and guests use every day.

See how Comcast Business can help.

LEARN MORE