

# Digital Security

# 101

For Small Businesses



intel<sup>®</sup>



# Contents

## Help Protect Your Data

- 04 Network
- 05 Website
- 06 Wi-Fi
- 07 Accounts

## Help Secure Your Team

- 09 Enlist Your Employees
- 10 Protect Their Devices
- 11 Practice Safe Email
- 12 Refresh Your Tech
- 13 Adopt an End-to-End Strategy

## Get Started Today

- 15 Get a PC Made for Business
- 16 Step Up Your Security Strategy with Minimal Effort
- 18 Next Steps

# Introduction

**If you're a small business,** you probably work very hard to keep your customers happy. But good customer service goes beyond a friendly hello or prompt service. Today, the most forward-thinking companies are taking measures to protect the sensitive data entrusted them by customers.

When approximately 43% of data breaches target small businesses<sup>1</sup> at an average cost per breach of \$101,000<sup>2</sup>, it goes without saying that security should be an essential part of any business strategy. But having a dedicated IT security position on staff doesn't have to be.

In this document, we'll outline a few basic steps businesses of any size can take to help protect their employees, their customers, and the bottom line.

# ■ Help Protect Your Data

**77% of SMBs** worry they will be the target of an attack in the next 6 months.<sup>3</sup>

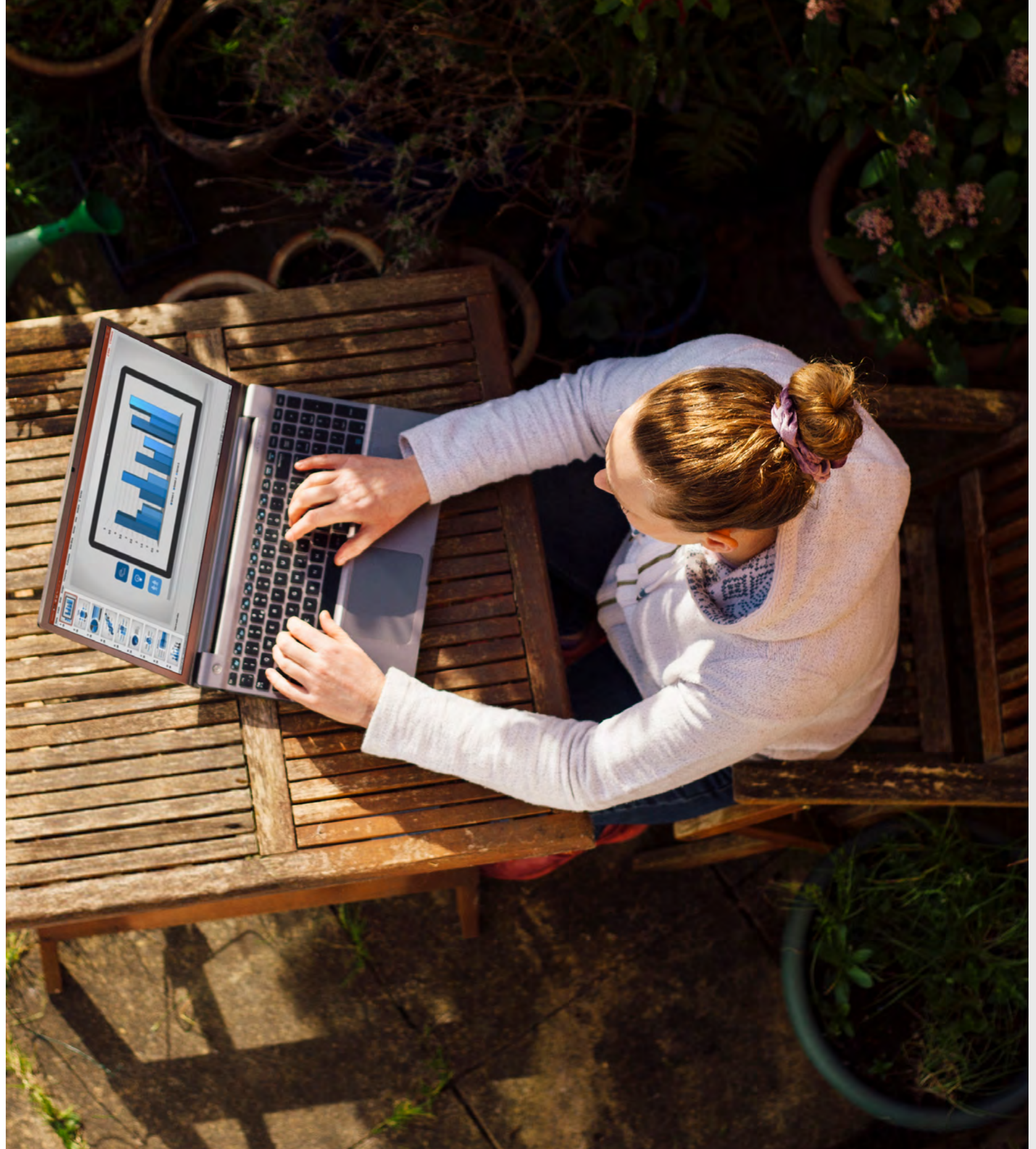


# Network

Network threats are continually evolving. You can stay ahead of today's attackers with innovative security solutions that can help detect, analyze, and block advanced threats like ransomware before they reach your employees on the web, email, and social platforms.

## TIPS

- Keep your machine clean by always having the most **up to date versions** of your security software, operating system, and web browser.
- Be sure a **firewall** is in place to keep your network private.
- **Regularly backup** all important business info and store offsite or in the cloud.
- Adopt a **hardware-based security strategy** to help protect against evolving threats.



# Website

Ideally, security procedures should be integrated into your website as it's being planned and developed. After development, performing regular penetration tests and vulnerability scans against your websites is a must to detect critical security issues before real hackers do.

## TIPS

- **Limit the amount** of sensitive information uploaded to your site **and encrypt** all that is uploaded.
- Remove or disable any unnecessary services on your server.
- Regularly **backup all site data** and store offsite or in the cloud.
- **Update all server software** to the most up to date versions.



# Wi-Fi

If you offer Wi-Fi to employees or visitors, be sure it is secure and protected.

## TIPS

- Offer **separate networks** for employees and anyone else needing internet access.
- The employee **network should be encrypted**, network name not broadcasted, and the network restricted to specific devices.



# Accounts

Without a dedicated defense, like an IT or security department, small businesses are an easier target for cybercrime. Your first line of defense is a strong password protected by two-factor authentication. Without that, websites you use to power your business—email, e-commerce, accounting, even social media—are prime targets for a takeover.

## TIPS

- **Use strong and unique passwords** for each account. (A password manager may help relieve the burden of remembering them all.)
- **Don't share your passwords** between employees on chat or email. (Password Managers also provide secure ways to share passwords between employees.)
- Add additional layers of authentication on as many accounts as you can. Go to [passwordday.org](https://passwordday.org) to learn more about Layering Up your Logins.



- Help Secure Your Team







# Enlist your employees

The old cliché “a chain is only as strong as its weakest link” is very true when it comes to security. Company employees (and even CEOs) have replaced software exploits as attackers’ favorite way to infiltrate your business. Enlist your employees in the cause. And make security a part of your workplace culture.

## TIPS

- Develop an **ongoing education program** that covers the security basics for passwords, email, browsing, and social engineering.
- Run weekly, ongoing **phishing simulations**.
- Send regular reminders of security topics and **company security policies**.
- Consider adopting **password management software**.



# Protect their devices

Most small businesses use mobile phones, laptops, and tablets as a way to increase employee productivity. Although extremely convenient, they can offer a significant potential threat. Mobile devices are often lost or stolen which can lead to data loss or a security breach. Policies and procedures need to be put in place to increase mobile device security.

## TIPS

- Password protect and **install security software** on every mobile device that has any company email or information.
- Encrypt **mobile device data**.
- Have **reporting procedures** in the event of a loss.
- **Deploy remote manageability software** for easy troubleshooting and faster recovery.

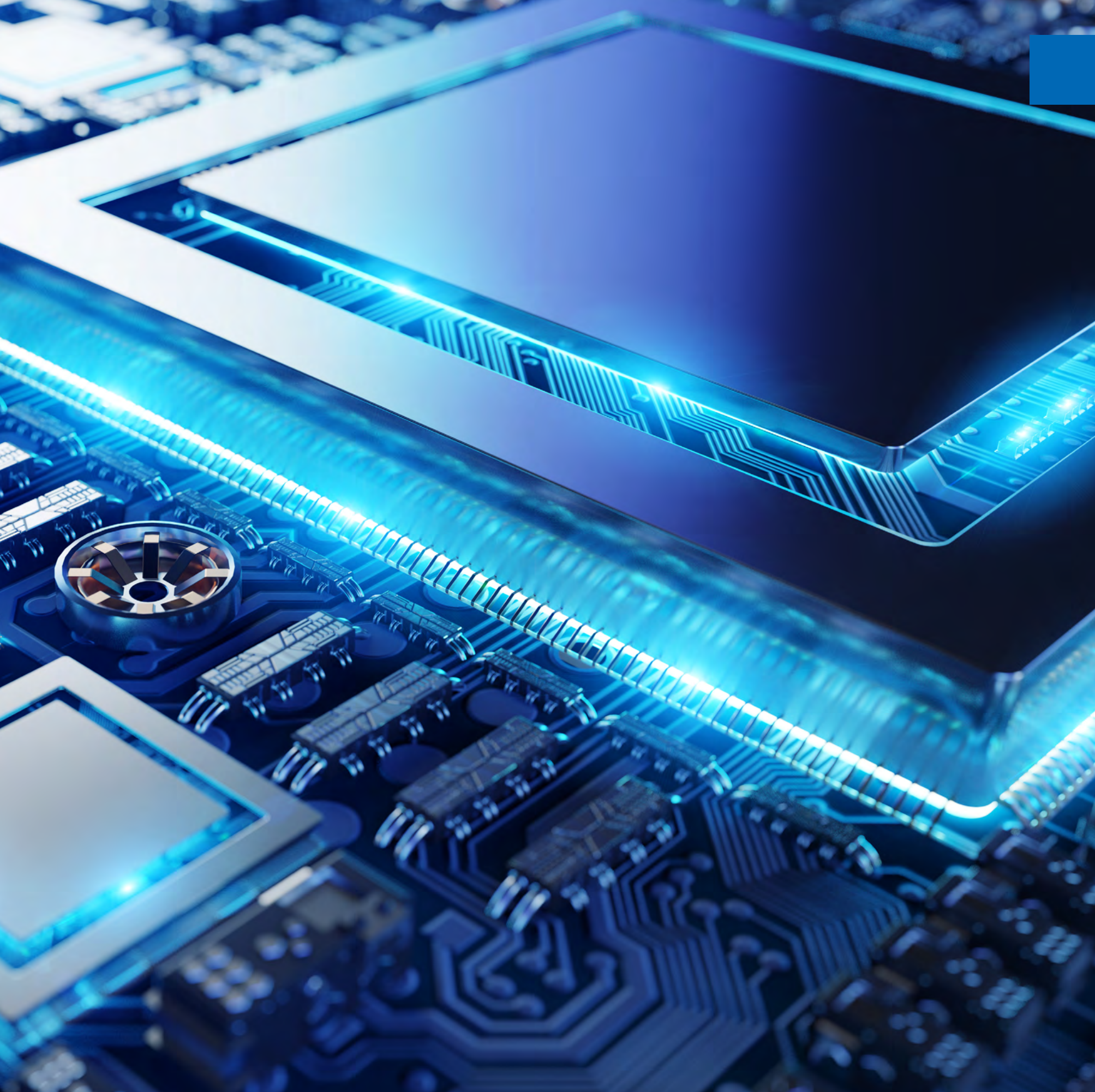


# Practice safe clicking

Most cyber attacks require a user to click something: a malicious link in an email or text, the install button of a virus disguised as legitimate software, or just a dangerous attachment. It is estimated that approximately half of all email is spam, phishing attempts, or other unwanted messages<sup>4</sup>. It is the most prevalent way of spreading malware and imperative that precautions are taken to keep it safe and secure.

## TIPS

- **Install security software** to automatically identify and block malicious messages.
- Enable **email encryption**.
- Create policies for employees on how to **identify safe and unsafe links** in email or on the web.



# Refresh your tech

A Microsoft study concludes that the optimal age of PCs is 4 years old, beyond which the cost of repairs and lost productivity makes them cheaper to replace.<sup>5</sup> If it's time to refresh your company's tech, make sure you consider the hardware security features that computer and server manufacturers are offering.

## TIPS

- Look for **hardware security features** like secure biometrics, built-in 2-factor authentication, and secure enclave technology built into the computer's processors.
- **Consumer Reports** now measures the privacy and security of the products, apps, and services they review. Make sure to use this resource to help inform your purchasing decisions.



# Adopt an end-to-end strategy

Flexible work is here to stay. In a recent Microsoft survey, 73% of workers said they want flexible work to continue.<sup>6</sup> More remote work means more digital touchpoints, which give attackers new opportunities to breach your business. Sophisticated threats such as worms, ransomware, cryptomining, and trojans have evolved to bypass traditional security and potentially destroy your local or cloud-based backup. The average time to identify a breach is 197 days and to contain one is 69 days.<sup>7</sup> It's essential to take steps to defend your business.

## TIPS

- Recognize that **anti-virus software is not enough**. Adopt a comprehensive, new security approach to reduce the attack surface and build your defenses.
- **Prioritize hardware-based security solutions** that help protect against attacks, detect them when they happen, and quickly recover afterward.

# ■ Get Started Today

“Better be despised for too anxious apprehensions, than ruined by too confident security.”

**Edmund Burke**

Author and Political Theorist



# Get a PC made for business

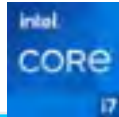


**Intel business PCs can help your business get a robust security strategy, right out of the box.**

The Intel vPro® platform and Intel® Core™ processor-based business PCs help boost your business's digital security with robust, hardware-based security features that help to protect against attacks, detect them as soon as they happen, and enable swift recovery in the event of an attack.



# Step Up Your Security Strategy with Minimal Effort

Consider Intel vPro®-based PCs as your starting point

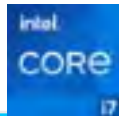


	 Intel® Core™ Processors	 Intel vPro® Essentials	 Intel vPro® Enterprise
<b>Protect: Increased protection against emerging threats</b>			
Built-in below-the-OS security to help protect from firmware attacks at PC startup with BIOS Guard and Boot Guard	✓	✓	✓
Below-the-OS security features to help protect from advanced firmware attacks with Intel® System Resources Defense and Intel® Runtime BIOS Resilience		✓	✓
Help shut down an entire class of memory safety-related attacks which have long eluded software-only solutions with Intel® Control-flow Enforcement Technology (Intel® CET), now available on all 12th Gen Intel® Core™ and Intel vPro® devices.	✓	✓	✓
<b>Protect: Helping mitigate data breaches</b>			
Optimized to support running multiple workloads, apps and operating systems on one device with Intel® Virtualization Technology (Intel VT)	✓	✓	✓
Help protect sensitive OS data such as user log in credentials from malware attacks with Intel® VT-x	✓	✓	✓
Help protect critical data and secrets in the OS from advanced firmware attacks with Intel® Trusted Execution Technology (Intel® TXT)		✓	✓
Complete below-the-OS security visibility for better security and access management policies with Intel® System Security Report		✓	✓
Help protect devices and data from physical tampering attacks through hardware-based memory encryption with Intel® Total Memory Encryption (Intel® TME)		✓	✓
Advanced protection to help protect data in memory through extensive DRAM encryption with Intel® TME - Multi-Key (Intel TME-MK)**			✓
Help protect against remapping attacks that can compromise the OS with Intel® VT-rp**			✓

\*\*Dependent on future OS adoption



# Step Up Your Security Strategy with Minimal Effort

Consider Intel vPro<sup>®</sup>-based PCs as your starting point

	 Intel <sup>®</sup> Core™ Processors	 Intel vPro <sup>®</sup> Essentials	 Intel vPro <sup>®</sup> Enterprise
<b>Detect: Enables continuous detection of advanced threats*</b>			
Silicon-enabled AI threat detection to better detect ransomware and cryptojacking attacks with Intel <sup>®</sup> Threat Detection Technology (Intel <sup>®</sup> TDT) - Ransomware & Cryptominers	✓	✓	✓
Implement security strategies and boost security capacity with uncompromised employee productivity with Intel <sup>®</sup> TDT - Advanced Memory Scanning	✓	✓	✓
Monitor business applications and identify early indicators of attacks in real time with Intel <sup>®</sup> TDT - Anomalous Behavior Detector	✓	✓	✓
<b>Recover: Minimizing critical downtime in the event of an attack with remote PC support &amp; management</b>			
Support capabilities to remotely access the BIOS to troubleshoot in the event of an attack with Intel <sup>®</sup> Standard Manageability/ Intel <sup>®</sup> Endpoint Management Assistant (Intel <sup>®</sup> EMA)		✓	✓
Comprehensive support capabilities for employees with advanced recovery features—even when the operating system is down with Intel <sup>®</sup> Active Management Technology (Intel <sup>®</sup> AMT)/Intel <sup>®</sup> EMA			✓
Graphical control of remote devices even when the OS is down, enabling an efficient and prompt recovery with Intel <sup>®</sup> AMT/Intel <sup>®</sup> EMA			✓
Remotely remove all sensitive data from an infected PC <sup>1</sup> , helping reduce the impact of an attack with Intel <sup>®</sup> AMT/Intel <sup>®</sup> EMA			✓
Remotely reinstall OS on compromised systems post cyberattack, saving time and money with Intel <sup>®</sup> AMT/Intel <sup>®</sup> EMA			✓

\*Requires security vendor enablement.

<sup>1</sup> Requires OEM enabling. Additional steps may be needed to enable specific OS recovery.

# Next Steps

Feeling overwhelmed?  
Here are some resources.

**If you don't know where to start with improving your business' online security, check out these resources, or find an expert in security and privacy for small businesses.**

- Intel's [Digital Security Page](#) has great information on protecting your logins.
- [The Small Business Association](#) has a wonderful cybersecurity tool to kickstart your cybersecurity plan.
- [The National Institute of Standards and Technology](#) also has small business cybersecurity on lock. Check out their comprehensive guide to all things security [here](#).
- [Consumer Reports](#) is a great resource when upgrading your hardware to the latest technology. They now rate products for security and privacy.

# Sources

- 1 PurpleSec, "2021 Cyber Security Statistics The Ultimate List of Stats, Data & Trends," 2021.
- 2 Kaspersky, "Investment adjustment: aligning IT budgets with changing security priorities," Q3 2020.
- 3 Connectwise, "The State of SMB Cybersecurity in 2020: Creating Opportunity from Adversity," Sept 2020.
- 4 Infosecurity Group, "Half of Global Emails Were Spam in 2021," Feb 2022.
- 5 Microsoft. "True cost of not replacing computers revealed in Microsoft study: more than \$4,000 each," Oct 16, 2018.
- 6 Microsoft, "2021 Work Trend Index: Annual Report – The Next Great Disruption Is Hybrid Work — Are We Ready?," March 2021.
- 7 Varonis "Data Breach Response Times: Trends and Tips," Jun 2020.

# Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more at [Intel.com/PerformanceIndex](https://www.intel.com/PerformanceIndex).

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See Performance Index for configuration details.

Certain features available on select SKUs only. Please check OEM or retailer website for specific device details.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.  
© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.  
Other names and brands may be claimed as the property of others.

intel<sup>®</sup>