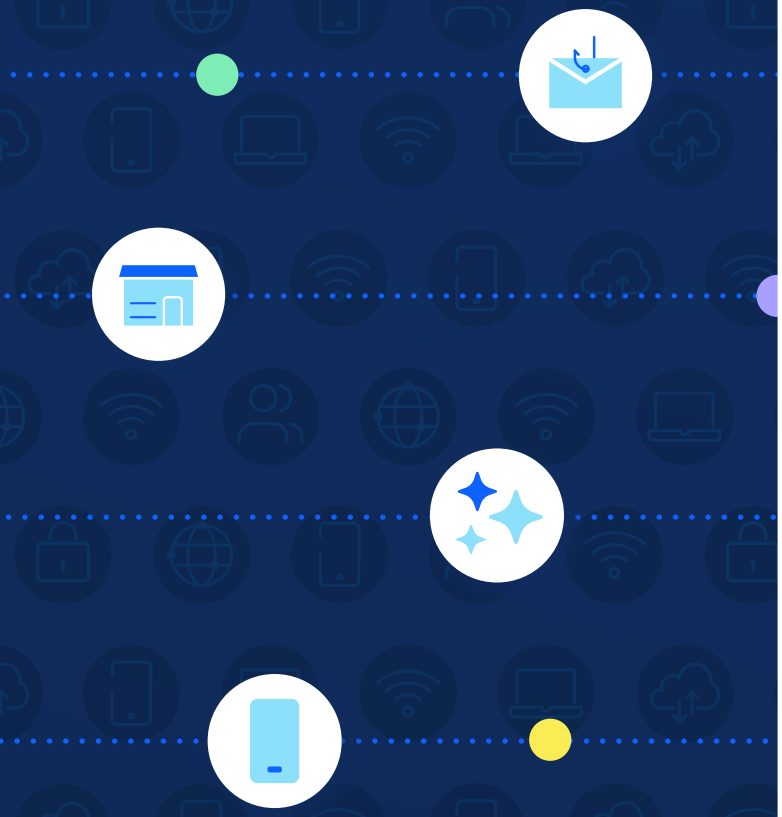
2024 Comcast Business

Small Business Cybersecurity Report

COMCAST BUSINESS

Since 2022, Comcast Business has conducted an annual review of anonymized threat data gathered from our SecurityEdge™ service and has issued our *Comcast Business Small Business Cybersecurity Report*.

This third annual Report reviews data from July 2023 to June 2024. It offers a window into some of today's threats, and how our service, supported by threat intelligence derived from AI-driven analysis of terabytes of data per day from our partner Akamai, can help deter them.



Key Takeaways for Small Businesses

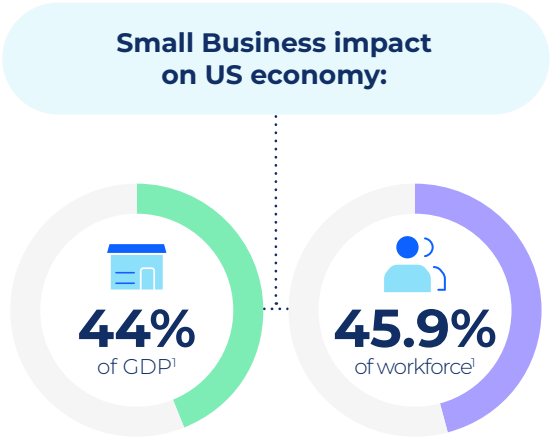
- **Dramatic reports of ransomware attacks get a lot of media coverage** — Most of them start with phishing.
- **Small businesses can be vulnerable** because they may lack specialized security resources. Even modest losses and loss of customer trust can impact small businesses.
- **Artificial Intelligence (AI) is a powerful and useful technology**, but it is also helping hackers and threat actor groups dramatically increase the number and effectiveness of attacks.
- **Mobile phones can also be vulnerable** to security incidents that compromise critical business data.

Cyber Threats Pose Big Risks to Small Businesses

Small businesses have a big economic impact

Since media reports about internet threats often cover large-scale incidents targeting enterprise-level businesses, some may think smaller businesses aren't affected. But today, it's easier than ever for hackers to target companies of all sizes.

Small businesses have a massive impact on the US economy. They generate nearly 44% of GDP and employ 45.9% of Americans — 61.6 million workers.[1] Small businesses are also major participants in supply chains, as both producers and consumers. Given their strategic importance, small businesses need to act to help protect themselves against internet threats.



Cyberattacks and Your Bottom Line

Early cyber threat actors saw big opportunities in larger organizations with more cash, data, and workers to target. As their tools have become more sophisticated, cyber criminals have diversified their efforts and today see opportunities with small businesses that are focused on running their operations and do not have dedicated IT teams.

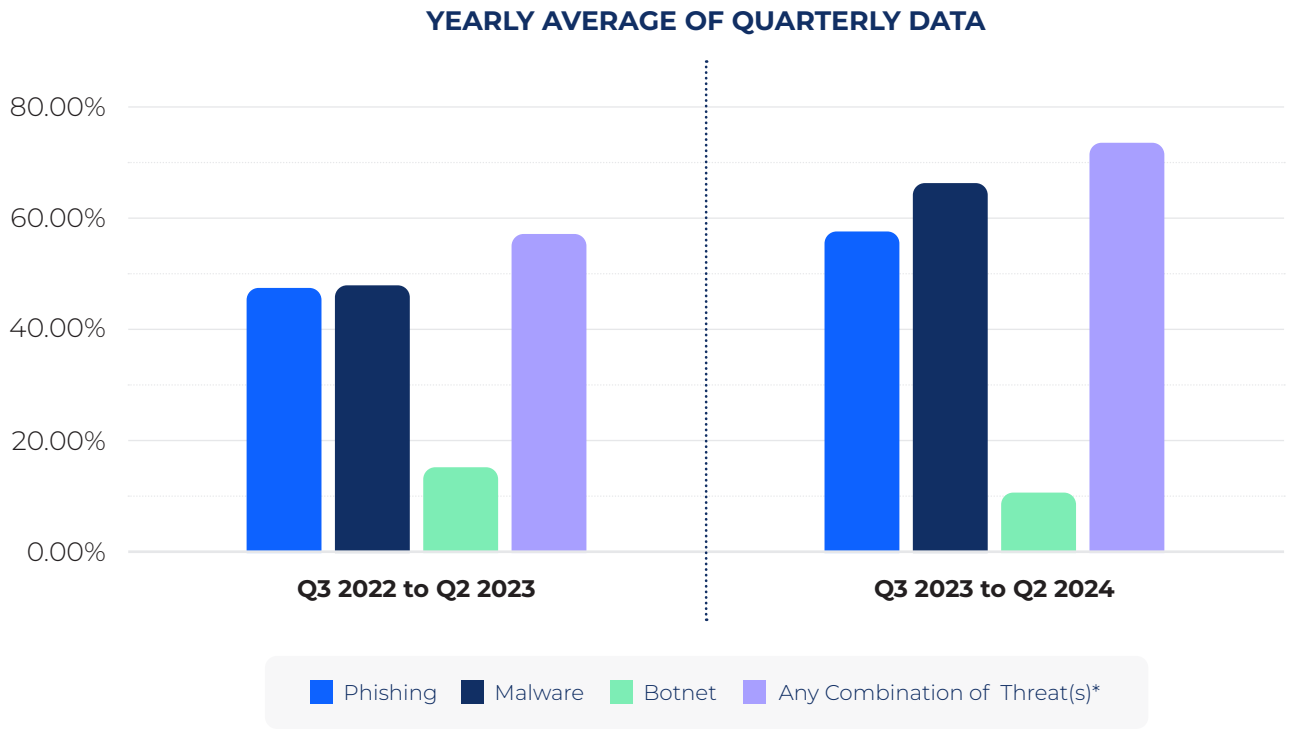
Evidence of this is seen in the Internet Threat Research Center (ITRC) *2023 Trends in Identity Report*. It shows a 28% increase in cyberattacks experienced by small businesses compared to 2022. **The report also showed of those small businesses that reported a cyber event: 42% reported revenue loss, 32% reported loss of customer trust, and 32% reported regrettable employee turnover following their cyber events.**[2]

These trends should prompt business decision makers to better understand the internet threat landscape and the risks threats pose, especially as attackers leverage new technologies like AI and automated services that make it easier than ever for them to launch their exploits.

1. U.S. Chamber of Commerce Small Business Data Center: https://www.uschamber.com/small-business/small-business-data-center
2. ITRC Business Impact Report: https://www.idtheftcenter.org/publication/itrc-2023-business-impact-report/

SecurityEdge™ Helps Protect Small Businesses

Twelve months of SecurityEdge™ data from Q3 2023 through Q2 2024 shows the percentage of businesses defended from different kinds of threats. As attackers have extended their focus beyond large organizations, exposure for small businesses has increased.



Comcast Business SecurityEdge™

LEARN MORE

*Restrictions apply. Not available in all areas. SecurityEdge™: Requires Comcast Business Internet and leased router for additional monthly charge. Will not work if connected via public WiFi, and may not work if connected via Connection Pro, virtual private network technology or non-Comcast DNS servers.

2024 Threat Landscape

Comcast Business gathers anonymized insights on cyber threats from small businesses with its SecurityEdge™ service, which is powered by Akamai with global visibility into anonymized internet traffic across a broad array of industries. Akamai researchers are focused on helping to defend against fast-moving attackers with automated tools that make it easier for them to innovate and expand their base of targets.

This is the third *Comcast Business Small Business Cybersecurity Threat Report*. Comparing high-level data from the 2023 report to 2024 data:

DAILY AVERAGE BLOCK ACTIVITY

Malware

↑ 349%*

Increase

In November 2023, there was a spike in activity intended to mimic software downloads. Numerous campaigns were observed supporting tools hackers use to distribute ransomware and banking malware.

Phishing

↑ 7.9%*

Increase

It was steady over the first part of the year and picked up starting in spring of 2024. Activity targeting many business services - shipping, payments, banking, communications, online storage and many more – was observed.

Botnet

↑ 368%*

Increase

A spike of activity in the spring of 2024 contributed to the rapid growth. Bot activity that supported malware downloads and Distributed Denial of Service (DDoS) attacks was most prevalent.

Data from Q3 2023 to Q2 2024 showed:

Highest number of blocks from suspected malicious activity in a single day	Highest number of businesses benefiting from SecurityEdge™ defenses in a single day
807,381,202 Potential accesses to web destinations hosting **malware**	**155,595** Prevented from accessing malicious websites
30,795,046 **Phishing** attempts	**91,193** Defended against phishing
231,883,942 Instances of **bot** activity	**11,338** Defended against Bot activity

*Anonymized data gathered from the SecurityEdge™ service captures blocked malicious DNS queries in each of the three threat categories. Automated exploits can generate extremely high query volumes.

An Inside Look at Cyber Threats

Businesses of all sizes use online services for payroll, marketing and other critical functions. Unfortunately, threat actors use online services as well to automate the roll out of exploits so they can broaden their base of targets. Traditional organized criminal networks have also moved their operations online.

CYBERATTACKS:
The Terrible Three

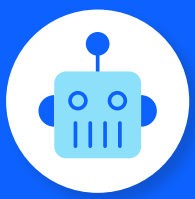
Phishing

Malicious web links in emails, texts, or other places designed to encourage clicks that take people to web sites where valuable personal information can be harvested and held for ransom or sold.

Malware

Malicious software unwittingly downloaded by users that is designed to locate and steal valuable data, encrypt data and demand payment, damage or disrupt devices, or gain unauthorized access to a network.

Botnets



Software secretly installed on computers and remotely controlled. Networks of bots find and upload valuable data, launch attacks, provide access to machines and more.

Stay Off the Hook: Ways To Avoid Phishing Attacks

Phishing remains a persistent problem and can lead to many types of cyberattacks. Businesses may go to great lengths to protect their network and data, but often, people are weak links in the cybersecurity chain. Threat actors abuse visible brand names and have become skilled at changing their strategies to manipulate our emotions and actions. Here are some common methods they use and ways to stop them in their tracks.

Look carefully for typos in domain names

- ✗ Remote.casinc.biz_casinc
- ✓ Remote.casino.biz_casino

Watch out for transposed letters or numbers

- ✗ login.moffice356.com
- ✓ login.moffice365.com

Check top-level domains (TLD)

- ✗ apple.bid
- ✓ apple.com

Check website name

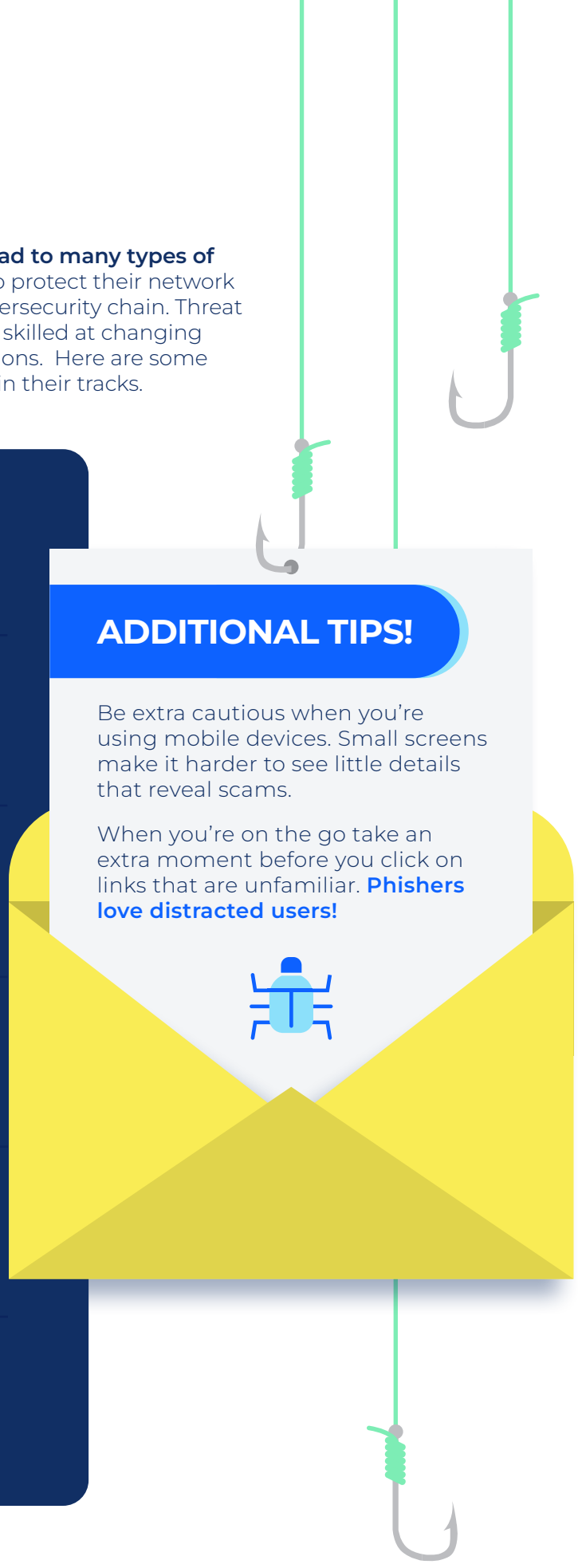
- ✗ apple.com.brlb.ru
- ✓ apple.com

Check for letters and numbers that look alike

- ✗ 0utlookwebaccess
- ✓ Outlookwebaccess

If something feels off, paste it into a search bar to see what happens

- ✗ googleplusforus.com — is not a Google web property



ADDITIONAL TIPS!

Be extra cautious when you're using mobile devices. Small screens make it harder to see little details that reveal scams.

When you're on the go take an extra moment before you click on links that are unfamiliar. **Phishers love distracted users!**

Cyber Threats Are Evolving with Emergence of Artificial Intelligence (AI)

AI is an incredibly promising and productive technology with far-reaching impacts. Unfortunately, widely available AI tools help cyber criminals craft compelling content for phishing emails, texts, social media posts and other purposes. Unlike some of the crude attempts and poorly phrased scam messages of the past, AI-developed tools and messages are more sophisticated and believable than ever. Even the savviest of computer users can fall victim to realistic looking and sounding AI-developed scams.

Bad actors with limited skill can also move beyond generic mass market emails by analyzing online data about businesses and individuals to create phishing lures that are highly targeted and astonishingly real. AI also helps threat actors automate their exploits to address a wider swath of targets in a more manageable way. These AI and automated tools help phishing grow. Indeed, the Anti-Phishing Working Group, an independent nonprofit security research organization, reported 2023 was the worst year on record for phishing.[3]

ARTIFICIAL INTELLIGENCE: A POWERFUL DEFENSE TOOL

AI can equip powerful computers with special algorithms so they can do things that normally require human intelligence. With AI, computers can learn, recognize patterns, solve problems, and make decisions. In some cases, they can see patterns and connections in data that humans miss. Generative AI tools allow users to ask a question as if they were talking to a person, and get an answer generated by a computer. These new tools are incredibly easy to use and can create high-quality content like emails, realistic images and videos, or even term papers for students.

Security researchers use AI tools to help thwart cyber actors. Teams at Akamai built sophisticated AI-based algorithms, refined over many years, to identify malicious activity quickly and efficiently. These strategies are designed to help defend against increasingly agile attackers. They're also useful for keeping up with innovations that make it easy for cyber attackers to change the face of exploits and avoid detection.

3. APWG Phishing Attack Trends Report – 4Q 2023 https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf

Mobile Devices Can Be Especially Vulnerable to Attacks

Mobile phones and other portable devices have become essential tools for all kinds of job functions, for all kinds of businesses. Businesses recognize the value of the flexibility and productivity enabled by mobile devices, but these devices also can be exposed to security incidents.

Threat actors have noticed. According to Forrester Research, an information technology analysis firm, employee-owned and company-owned mobile devices are common targets in external attacks.[4]

Mobile devices are often overlooked from a security standpoint because there is a tendency to think they are not used to store business-sensitive information. However, threats can come when mobile devices access business data stored in the cloud. If attackers gain access to a phone, or to logins stored on a phone (username and password), they may be able to obtain valuable business information.

Akamai data from their mobile security service covering Q3 2022 to Q2 2024 showed **21% growth in exposure of mobile devices**. Even though there is more awareness of mobile threats, and more security features, we continue to see growth in this statistic.

4. Forrester Research The State Of IoT Security, 2023 https://www.forrester.com/report/the-state-of-iot-security-2023/RES179300

Comcast Business SecurityEdge™

Comcast Business SecurityEdge™ helps protect internet users and all their connected devices against threats such as malware, ransomware, phishing and botnets with advanced global threat intelligence powered by Akamai, which is updated every five minutes.

New features extend to help protect workers when they use PCs, mobile phones, or tablets away from the office. The service is easily managed through an internet customer portal and no additional equipment is required other than a compatible leased router.

The SecurityEdge™ Difference

Comcast Business SecurityEdge™ helps protect small businesses against increasing exposure to cyber threats. It is a simple, affordable and easy-to-manage cloud-based cybersecurity solution that actively identifies threats in Internet traffic and blocks end user access.

Agile Threat Intelligence

Automated AI-based processing of live-streamed network helps detect new threats. Malicious activity can be identified and rigorously validated in minutes.

Comprehensive Threat Coverage

With a focus on development of machine learning and AI algorithms, new exploits and subtle variants can be uncovered. Predictive analysis activates proactive threat entries to help deter future malicious activity.

Global Visbility

Anonymized production data sourced from networks all over the world and processed against a diverse array of threat indicators equip researchers to detect new threats and project their evolution.

FEATURES THAT WORK FOR YOUR BUSINESS

Easy set up, no extra equipment or software

All you need is Comcast Business Internet (or Ethernet Dedicated Internet, where available) and Comcast Business compatible leased router.

Visibility anytime and anywhere

See what is happening on your network by monitoring blocked threat activity via a personalized dashboard and email reporting.

Global Threat Intelligence updated every 5 minutes

Up to 90 different metrics are assessed to evaluate threats, and reputation scores are tracked to spot trends.

Content filtering and blocking

Businesses can set up personalized filters to block use of unwanted websites by employees and customers.

Comcast Business SecurityEdge™

LEARN MORE

COMCAST BUSINESS