COMCAST

2022 Xfinity Cyber Health Report

Insights about the state of cybersecurity in Americans' connected homes and tips for helping consumers protect themselves.

Secure Customers Are What Matter Most

A lot has happened since our last report in 2020. We've seen the pandemic change how we work with the rise of stay-at-home work, and then with the arrivals of vaccines and boosters bringing a new phase of hybrid work. All of these changes have continued to blur the lines between our professional and private lives, which - unknowingly to many - create new vulnerabilities and openings for cybercriminals.

We saw, yet again, with the pandemic that uncertainty opens new opportunities for bad actors as they look to turn global change into new ways to steal valuable information, identities and money. As we've seen the number of attacks and threat activity increase, the combination of today's connected homes and hybrid work environments present new cybersecurity challenges.

Today, our customers have an average of 15 connected devices per household – some as many as 34 – ranging from laptops, mobile phones and smart TVs, to connected door locks, baby monitors and even cars. But even as the number of devices and usage grows, our xFi Advanced Security service provides a protective shield for connected homes by blocking nearly 10 billion threats for our customers. The bottom line is, while the security environment continued to evolve, we stayed ahead of it and were effective against it, because nothing is more important to us than protecting our data, our systems, and most importantly, our customers from cyber threats.

That said, we know there is no silver bullet in cybersecurity, so we've always taken a multilayer approach to maintaining the highest security standards. As a result, our security program is built on three pillars that make us more resilient to change, even a global pandemic. These pillars include:

- **Secure Products** – We make cybersecurity a priority at every phase of the product development process, from inception to delivery. We call this approach "build security in." In contrast to the old approach of bolting security on at the end of the product development process, we integrate it into every phase, which results not only in more secure products, but also ensures that everyone at Comcast involved with supporting our customers is keeping security front-of-mind. We're excited to share how this comes to life in this report.

- **Secure Data** – We know that our customers' data is what the bad actors are after. That's why we endeavor to stay one step ahead by implementing innovative technologies for keeping that data secure. Our new threat intelligence platform is the most recent example of this – it enables us to analyze a massive amount of data to find and eliminate threats in a fraction of the time it takes when using conventional methods.

- **Secure Customers** – This will always be our "job 1." Keeping customers secure is what drives us. And I mean more than just keeping laptops secure; I mean keeping the whole household secure – from smart TVs and smartphones to gaming consoles and Wi-Fi-enabled appliances or anything that connects to your home Wi-Fi. We keep it all safe so our customers can enjoy all the benefits of their connected home.

To gain a better understanding of today's hybrid and connected home, and the security challenges that accompany it, Comcast commissioned its second Xfinity Cyber Health Report. This report includes a comprehensive survey showing how consumers approach cybersecurity for their homes and connected devices. We also provide some tips and recommendations on the things you can do to protect yourself, as well as information on some of our newer security innovations designed to layer more protection across our network.

We don't expect our customers to be cybersecurity experts. That's why we make a point of prioritizing security for them, from the gateway in their home through to the core of our network. I hope you find the report interesting and know that Comcast is continually innovating and watching over your security to protect your connected home and family – today, tomorrow and into the future.

Sincerely,

Noopur Davis
Chief Information Security and Product Privacy Officer, Comcast

We saw, yet again, that uncertainty opens new opportunities for bad actors as they look to turn global change into new ways to steal valuable information, identities and money.

2022 Xfinity Cyber Health Report

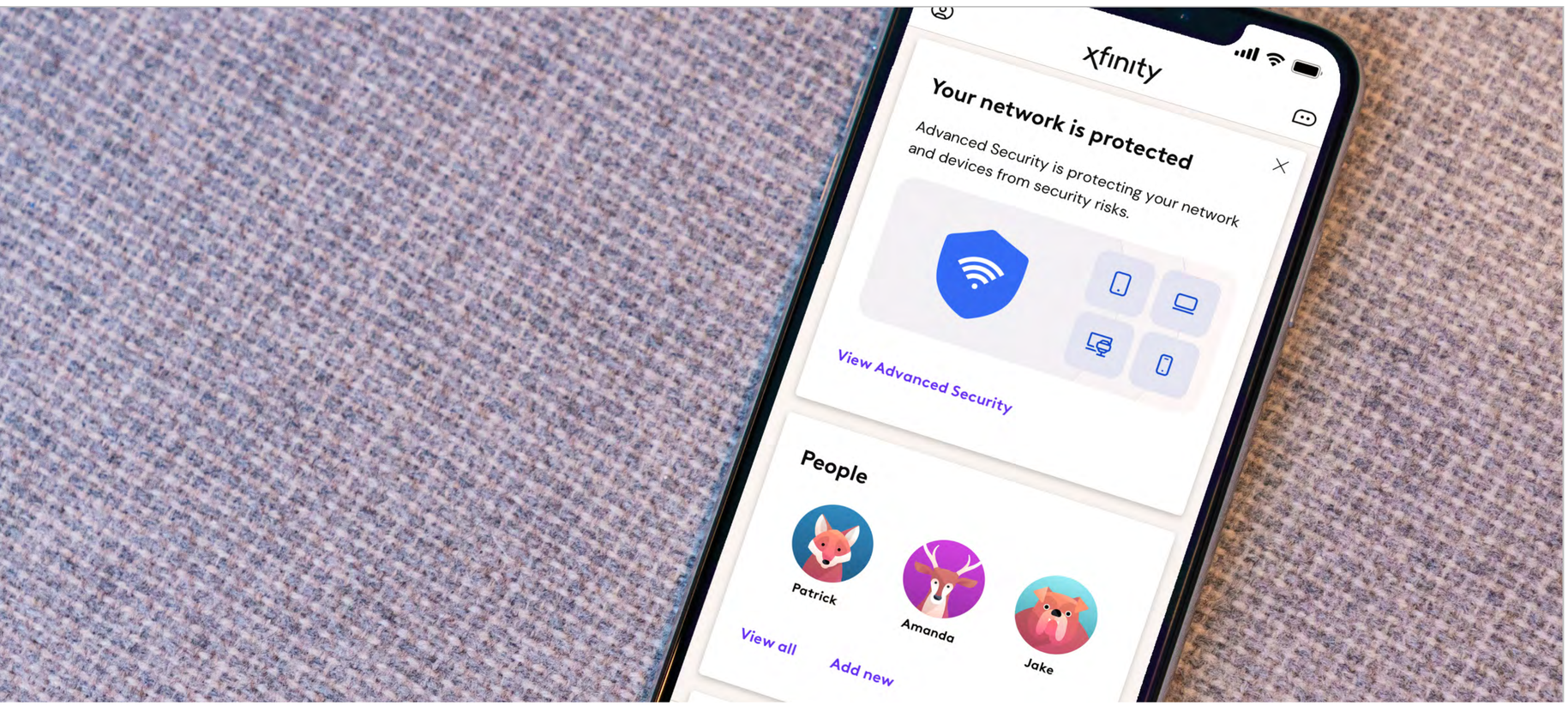
When we issued our 2020 Xfinity Cyber Health Report, the global pandemic was in its early stages. We were still adjusting to our newfound digital world – from working or studying from home to finding new ways to connect with friends and family without leaving the house – the internet quickly became the backbone of our daily lives. So, while our 2020 report revealed that consumers still had a long way to go when it comes to understanding cyber threats in the connected home and practicing cyber-safe behavior, the findings were understandable.

Here we are two years later, and while our reliance on the internet and demand for connected devices has continued to skyrocket – up to 12X since pre-pandemic levels – our 2022 survey findings demonstrate that progress in cyber-safe education and behaviors hasn't kept pace. In fact, it's remained stagnant or gotten worse – and there's a lot we need to learn and do to course-correct and protect our devices and connected homes.

Taking Connected Home Security Seriously

Research from International Data Corp. estimates smart home device shipments will reach $306.3 billion by the end of 2022, up nearly 6% from 2021. While connected home devices bring us many benefits, including convenience and control, they also introduce significant security risks. If left unprotected, bad actors can gain access to these devices and home networks where they can search for financial or other personal or sensitive information. Or, they may want to add connected devices to a "botnet" that's used to attack other people and organizations.

As the largest broadband provider in the U.S. serving more than 32 million internet customer households, Comcast defends against these types of attacks every day. To help protect our consumers, we made xFi Advanced Security, a feature that protects the home network from cyber threats, free to all of our internet customers with the xFi Gateway in January 2020. Since that time, we've blocked nearly 10 billion cybersecurity threats in customers' homes. While this is a significant step toward thwarting the attempts of bad actors, customers also need to do their part with practicing cyber-safe behaviors – because the connected home is here to stay and cyber attackers are becoming increasingly adept at infiltrating it.



12X

Increase in the number of connected devices in Xfinity households since before the pandemic

10B

Cybersecurity threats blocked by xFi Advanced Security in our customers' homes

Cyber Threats in the Connected Home: Consumer Knowledge and Practices

To gain a better understanding of consumer opinions, knowledge and practices around cyber security in the home, in November 2022, Comcast commissioned Wakefield, a market research firm, to conduct a survey of 1,000 nationally representative adults ages 18 and older. The following pages outline the results of our second Xfinity Cyber Health Report, including the threats targeting connected homes, where consumers are stacking up against these risks and where there's room for improvement.

74%

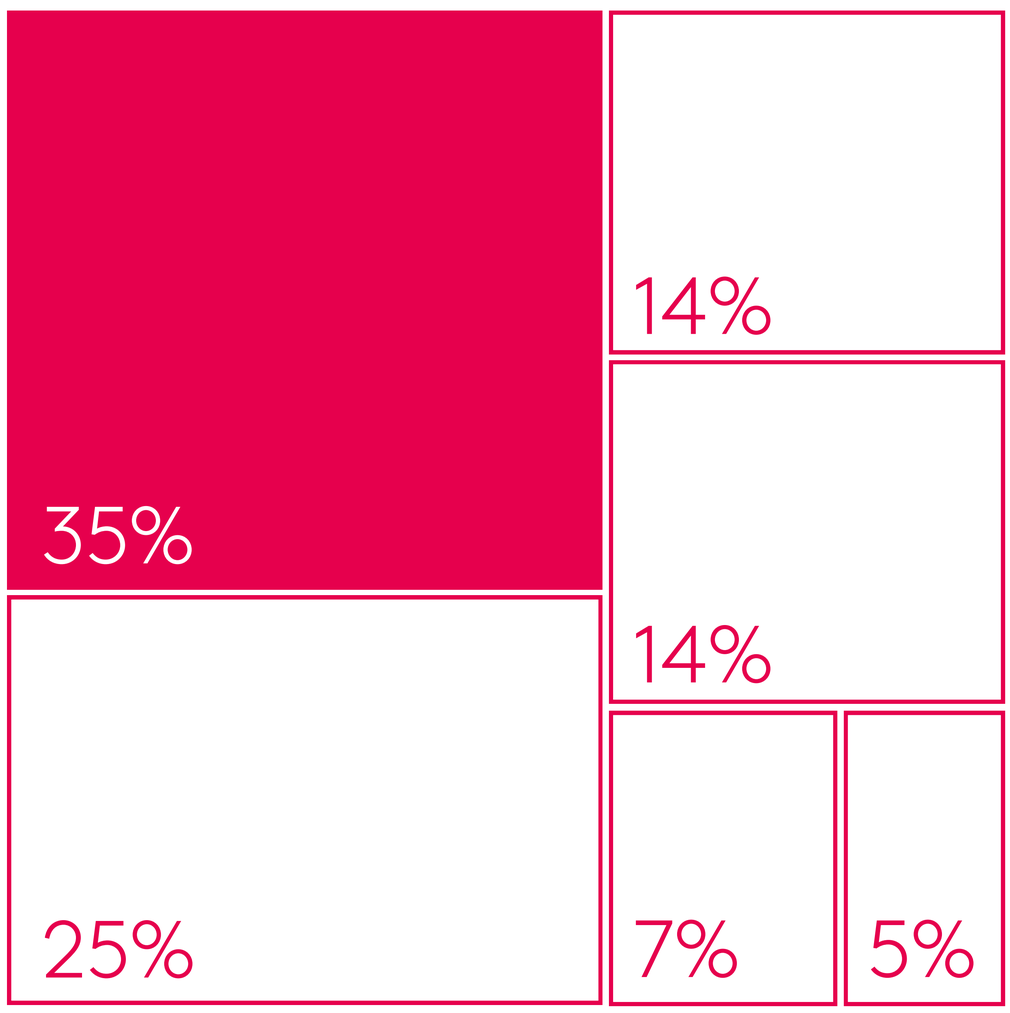
of consumers estimated less than 10 cyber threats hit their home network each month... in reality, consumers experience an average of 23 unique threats, with the total number 3-4x that due to repeat attacks.

The Threat Landscape: Perception vs. Reality

Similar to the 2020 report findings, respondents remain unaware of the large volume of threats targeting their home network each month. A quarter of survey respondents believe they aren't targeted at all by cyber threats, with an additional 49% noting they believe less than 10 attacks hit their home network every month. This is a stark contrast to the reality of the threat landscape.

Comcast's network data reveals xFi Advanced Security blocks an average of **23 unique threats each month – with the total number of attacks actually landing at three-to-four times that number, since many attacks are repeated** (note: xFi Advanced Security blocks all threats, but only counts unique attacks).

How many cyber-threats do you think hit your home network per month?



	2022
Zero (0) Threats	25%
1-4 Threats	35%
5-9 Threats	14%
10-24 threats	14%
25-99 Threats	5%
100 Threats	7%

Exactly what type of threats are consumers facing?

According to *xFi Advanced Security* data, the most common types of cyberattacks on connected homes are:

IP Reputation

This is when a known malicious external source tries to connect with a device in a consumer's home network.

Unsafe Browsing

This occurs when a user attempts to navigate to a website or is exposed to something on a website (e.g., an ad) that is known to be malicious.

Denial-of-Service (DoS) Attack

Bad actors launch large streams of network traffic from botnets to overwhelm networks and systems, so they become unavailable to users. Compromised connected home devices can be made part of these malicious botnets.

Model Profile

This happens when IoT devices become part of a botnet. A botnet, short for "robot network," is a network of hijacked computer devices used to carry out various scams and cyberattacks.

Remote Access

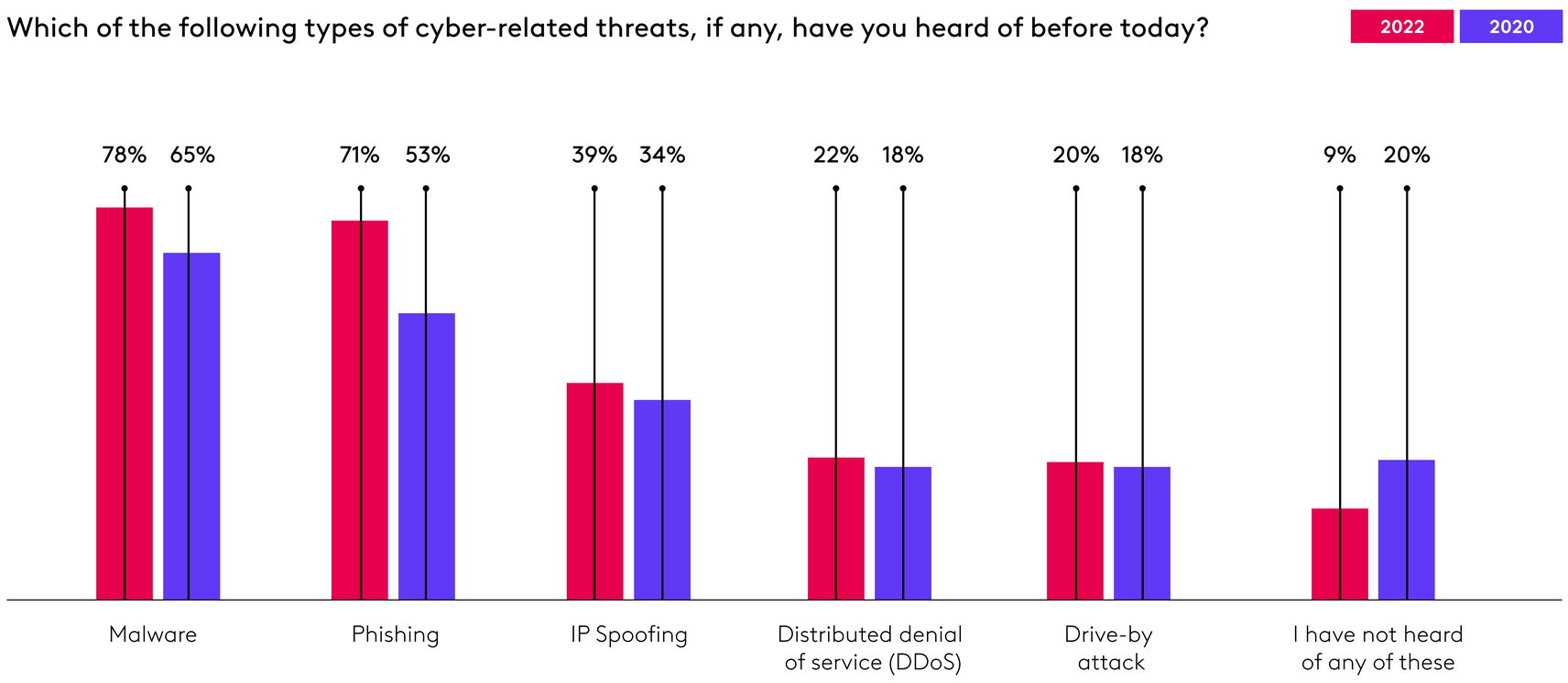
Malware designed to enable a bad actor to remotely infect and control a computer or system.

Cyber Threat Awareness and Understanding Improves

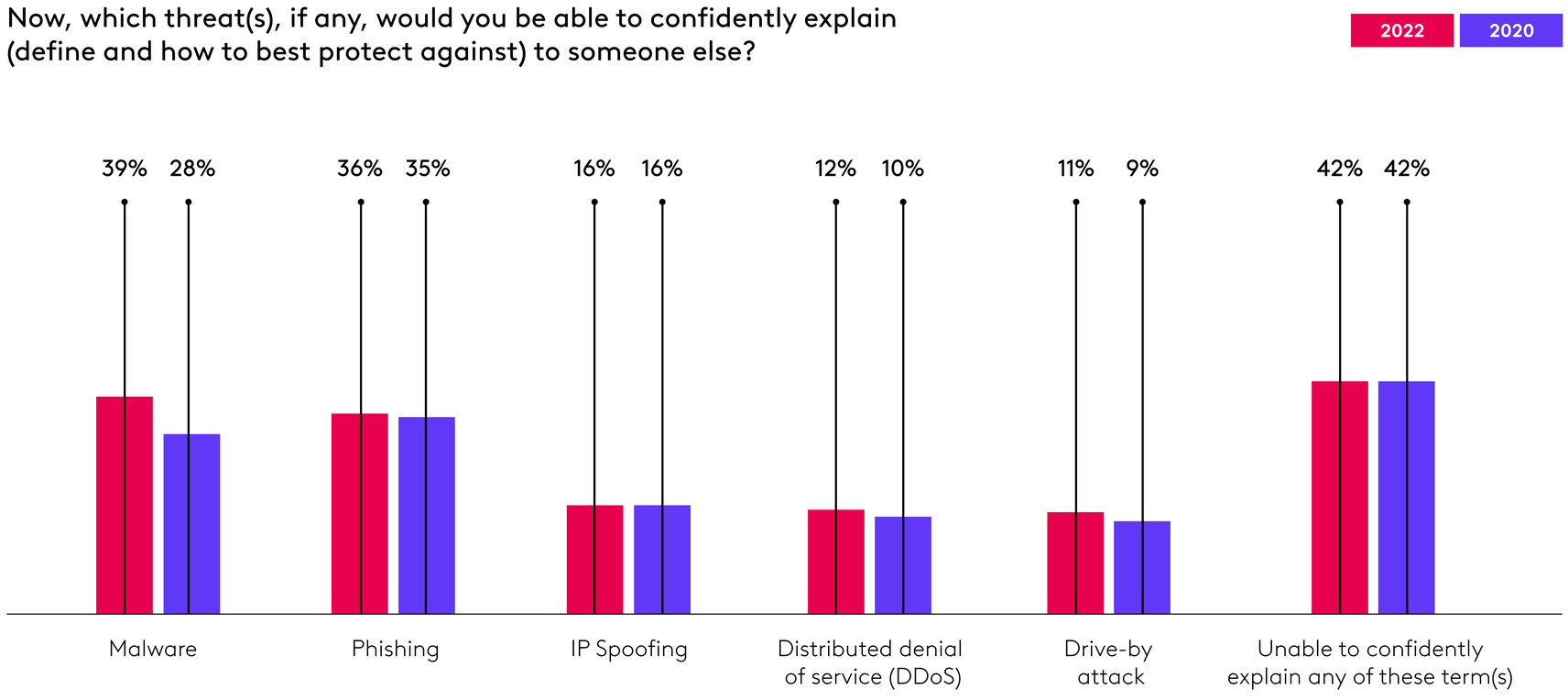
One area where consumers have shown progress since our 2020 report is in their level of knowledge about the various types of cyber threats. We saw improvement in both people's general awareness of threats and their understanding of how those threats work. For example, in 2020, 53% of respondents had heard of phishing, but only 28% believed they could confidently describe what it is. In our 2022 survey, 71% of respondents said they've heard of phishing, with 39% noting they'd be able to confidently explain it, representing significant gains in two years.

When it comes to general awareness and understanding of other types of threats, including malware, IP spoofing, distributed denial of service (DDoS) attacks and drive-by attacks, 2022 findings either improved or remained consistent with 2020 data.

Which of the following types of cyber-related threats, if any, have you heard of before today?



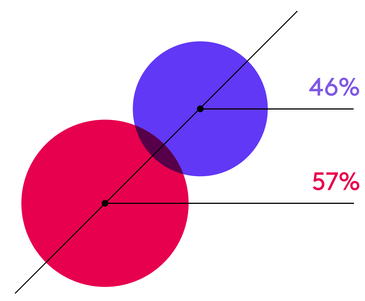
Now, which threat(s), if any, would you be able to confidently explain (define and how to best protect against) to someone else?



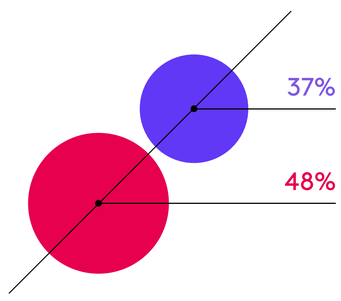
While this improvement in cyber threat savviness is certainly a step in the right direction, there's still more work to be done. When asked a series of six true or false questions about basic cybersecurity issues, 96% still got at least one wrong, with 41% answering three or more incorrectly.

Which of the following statements about cyber-related threats, if any, do you think are true?

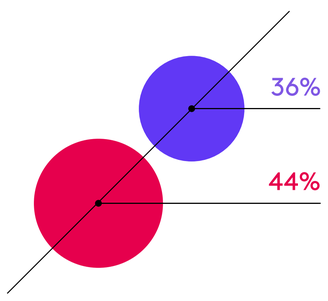
2022 2020



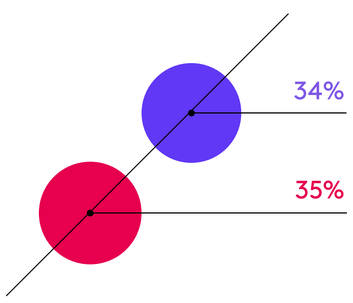
Viruses such as malware can sit on my computer, avoiding detection*



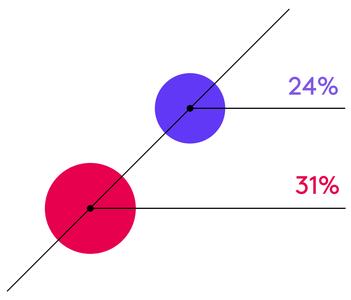
Most cyber-attacks begin with a phishing email*



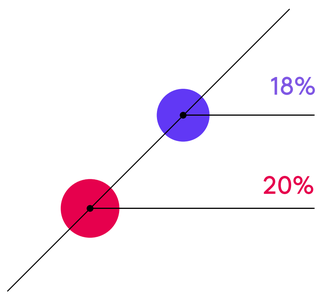
The longer the password, the more secure my device will be



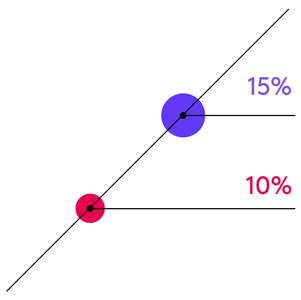
If my anti-virus software is up to date, I'm protected



Apple devices are less likely to get hacked than PC devices



Screen devices are more vulnerable to cyber-attacks compared to non-screen devices



None of these statements are true

96%

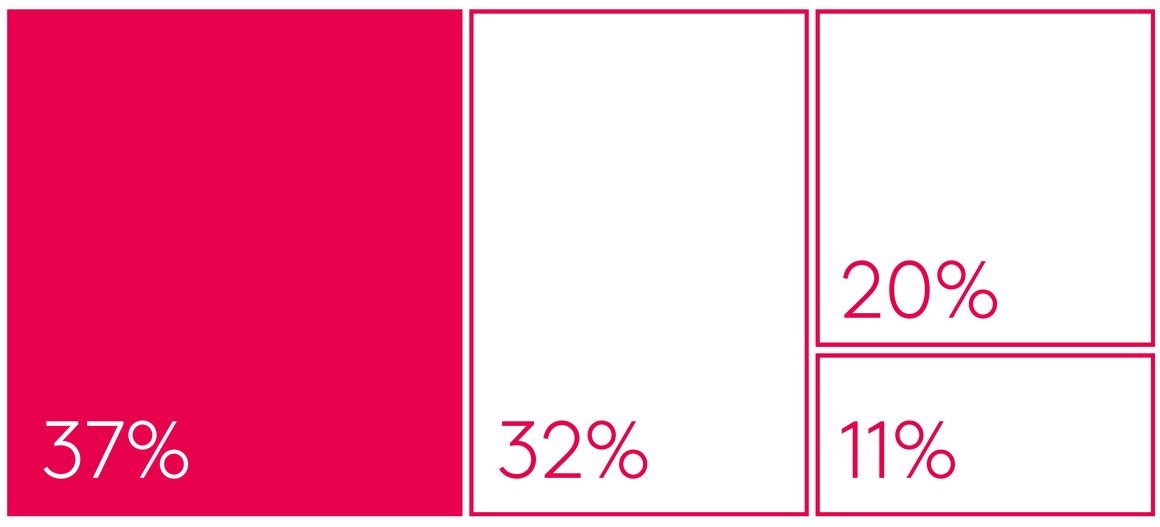
of consumers did not have knowledge of basic cybersecurity issues as they answered true/ false questions.

Cybercriminals Settle Into Unaware Houses

Being able to quickly identify a successful attack on a connected device or home network is critical in limiting the damage a bad actor can do and reducing the impact on your home and family. However, when asked how soon they would know whether they were a victim of a cyberattack, only 20% said immediately – leaving the remaining 80% vulnerable to having cybercriminals lurk on their network undetected for extended periods of time. In fact, **about a third (32%) of consumers said they aren't sure they'd ever know if they were a victim of a cyberattack**, introducing the potential for long-term security risks.

How soon do you think you would know if you were the victim of a cyber-attack?

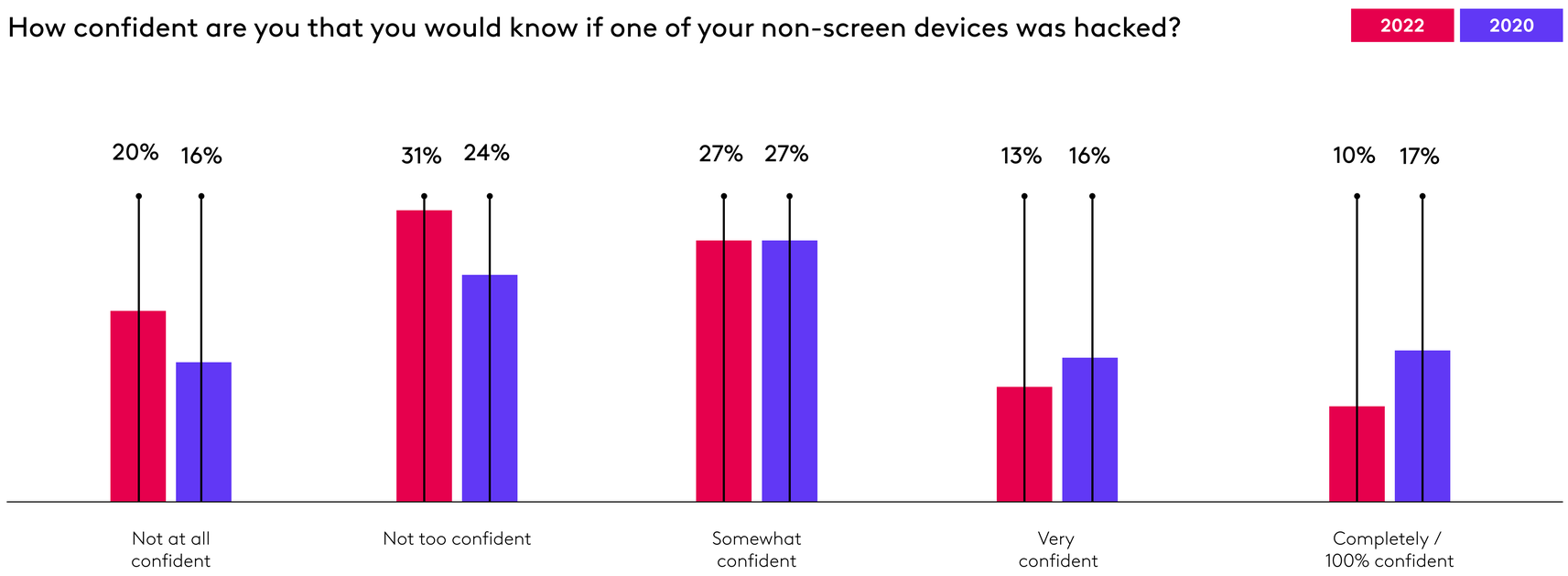
2022



When I notice something missing or not working	37%
I'm not sure I'd ever know	32%
Immediately	20%
When my internet service provider tells me	11%

An emerging challenge to awareness is that the connected home now includes a wide range of devices, some with screens and others without. In fact, **51% of respondents noted they are not really confident that they would know if a non-screen device was hacked**, such as a robot vacuum or a smart plug.

How confident are you that you would know if one of your non-screen devices was hacked?



Cybercriminals Target Expanded List of Smart Devices

And speaking of devices, when it comes to attack identification, it's also important to know which are most often targeted. When we compared real-world data from *xFi Advanced Security* regarding commonly targeted devices to survey data showing consumers' perceptions on the topic, we found that while consumers have a good understanding of the top two targeted devices – computers and smartphones – **they underestimate the risk associated with other connected devices**, including gaming consoles, streaming video devices, home security systems and even baby monitors.

We need to ensure all connected devices are secure, but any one of them can pose serious security risks. In fact, according to our network data, many emerging and unexpected devices fall on the commonly targeted list, including smart watches, lighting, thermostats, doorbells, garage openers, sports and fitness equipment, sprinkler systems and even cars!

What internet-connected devices are the most likely to give cyber-criminals access to a/your home network?

Device	*Consumers answered*
Computer (laptop or desktop)	61%
Smart phone	53%
Tablet	40%
Smart TV	27%
Voice assistant, such as Amazon Echo or Google Home	24%
Gaming console	23%
Streaming video device, such as Roku or Apple TV	18%
Home security system	15%
Smart watch	13%
Baby or pet monitor	12%
Smart hub	11%
Smart printer	9%
External hardware / storage	8%
Smart kitchen appliance, such as a refrigerator	6%
Robot vacuum	4%
None of these	6%

Most common devices actually targeted in 2022:

2022

Device	*# of threats*
Computer (laptop or desktop)	300,608,539
Phone	295,775,905
Generic, such as an IP camera	224,052,853
Unknown, such as storage devices, etc.	150,996,975
Network-Attached Storage (NAS)	141,299,860
Camera	77,139,922
Tablet	38,967,516
Router	22,753,110
Streaming video devices	19,967,456
Network device	19,182,466
DVR	18,301,209
Game console	14,506,389
WiFi extender	9,109,813
Smart TV	6,058,349
Set-Top Box	3,332,693
Ethernet Switch	2,317,818

‘Most unusual’ devices actually targeted in 2022:

Pets
Sprinkler system
Robot
Outlets
Kitchen appliance

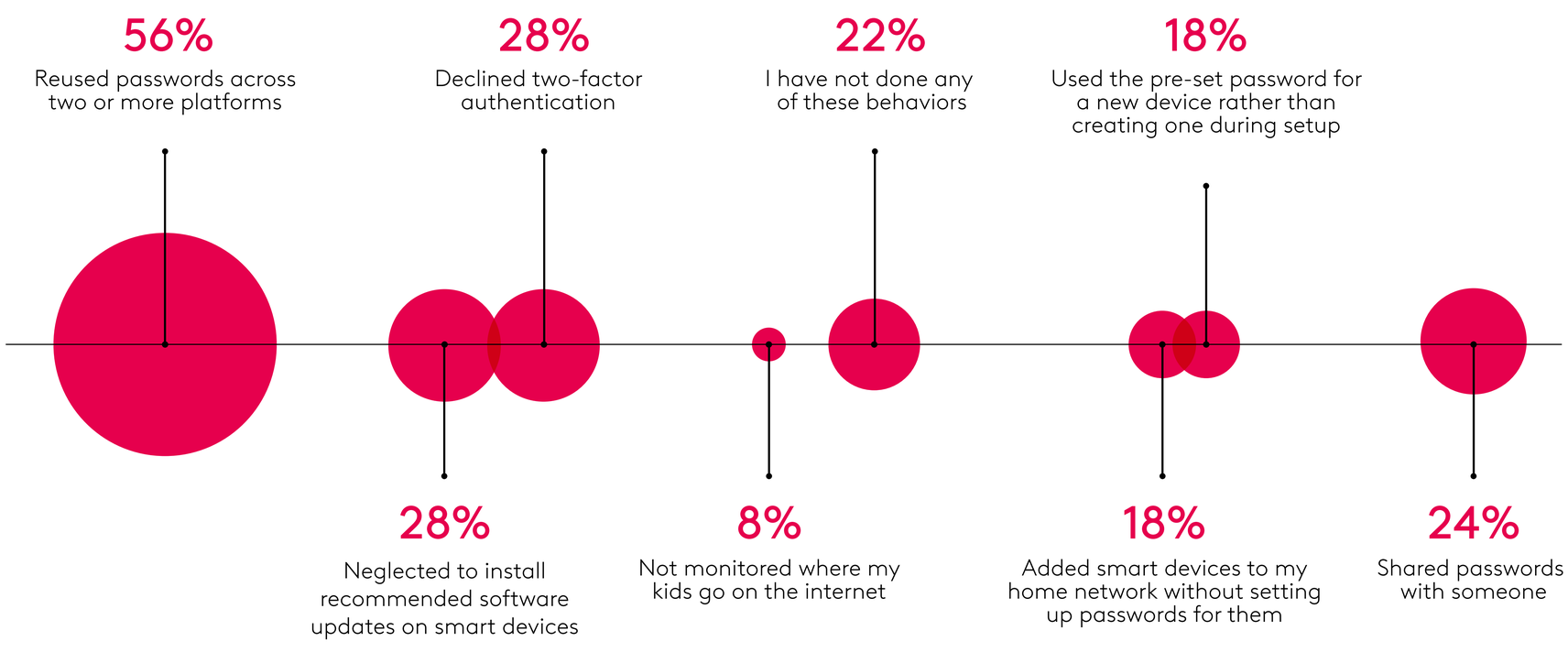
As Threats Rise, Consumer Cyber-Safe Behavior Has Declined

Consumers may have become increasingly savvy when it comes to cyber threats and how they work since our last report, but in a worrisome trend their cyber-safe behaviors declined over the same time period.

In fact, 78% of respondents admitted to risky behaviors that open themselves up to attack, including reusing passwords across two or more platforms (56%), neglecting to install recommended software updates on smart devices (28%) or even sharing passwords with someone else (24%). This combination of risky behaviors was up significantly from the last report when it was only 64%.

Have you ever, even once, done any of the following actions?

2022



The Connected Home Is Skyrocketing

Our survey reveals that Xfinity xFi customers are using more connected devices in their home than they were in 2020. Today, the average number of connected devices per household is 15, up 25% from 2020 – with "power users" having as many as 34 devices per household. And this trend is only expected to grow. In fact, 58% of survey respondents noted that they plan to buy at least one connected device during the upcoming holiday shopping season.

Which smart devices, if any, are you planning to purchase for your home during the holiday shopping season?

2022

26% Smartphone or tablet	12% Smart home security system	9% Smart fitness, sports equiptment, or tracker	7% Smart baby equiptment or device
16% Gaming console or accessory	12% Voice assistance, such as Amazon Echo	8% Smart toy, such as a robot or drone	5% Networked attached storage device
13% Smart appliance	12% Smart home tech, such as a light bulb or mirror	7% Smart pet equiptment or device	42% I do not plan on buying any smart devices during the holiday shopping season

58%

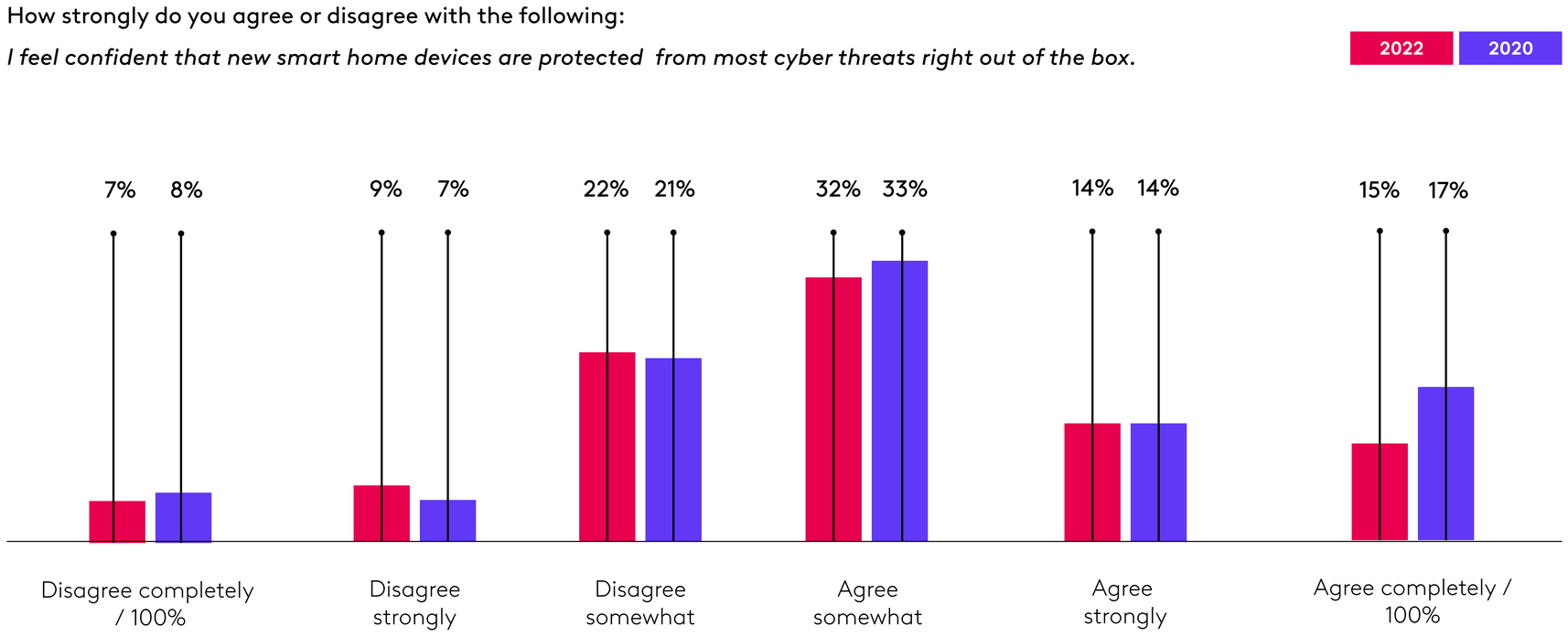
The total percent of people that think they will buy a smart device this holiday season

With the connected home rapidly expanding, consumers should educate themselves on the risks to their devices and networks, learn and implement security best practices and separate fact from fiction when it comes to security prowess.

For example, our survey also found that **61% of respondents either somewhat, strongly or completely agree that new smart home devices are protected from most cyber threats right out-of-the-box** – on par with the 65% who believed the same in 2020. Securing these devices at set-up and with on-going updates will become increasingly important as the average household continues to expand the number of connected devices they use.

How strongly do you agree or disagree with the following:

I feel confident that new smart home devices are protected from most cyber threats right out of the box.



A House Divided: Generational View of Cybersecurity

New for the 2022 report was a generational analysis of the responses across four major generations: Baby Boomers, Gen X, Millennials and Gen Z. The results in many ways reflect each generation's exposure and experience with technology as well as their stage of life, including:

Boomers Are the Safest Generation

In looking at risky cyber behaviors like sharing or re-using passwords or declining multifactor authentication, 70% of Boomers admitted to doing one or more of them. While that is a lot, it is still safer than Gen X (80%), Millennials (82%) and Gen Z (87%).

Millennials Are Device Shopping

77% of millennials are most likely to purchase a smart device this holiday season, which makes sense since they are likely the bulk of home buyers now. At the top of their shopping list: new smartphones, laptops and gaming consoles.

Gen Z Skipped Tech Class

In looking at the two highest profile styles of cyber-attacks, only 56% of Gen Z respondents had heard of malware before and only 38% had heard of phishing. These were both significantly lower than the next closest generation (Millennials, of which 72% recognized malware and 65% phishing) and also surprising given Gen Z grew up as digital natives surrounded by technology.

70%

of Boomers reported risky cyber behavior like sharing or re-using passwords, or declining multifactor authentication.

How Consumers Can Protect Their Homes

While consumers have made great strides in becoming aware of and better understanding various cyber threats to their connected devices and home networks, there is still more work to be done – especially when it comes to practicing cyber-safe behaviors.

The best defense against today's bad actors is a combination of following connected home security best practices and working with your internet service provider (ISP) to implement security offerings, because ISPs offer the "gateway" between the internet and your home network (for example, Xfinity xFi Gateway customers benefit from Comcast's xFi Advanced Security service). The following sections of this report will dive into both of these areas in much more detail, so you can protect your connected devices, your home network and your digital footprint.

Q&A: Securing Smart Devices in the Connected Home with Matter and xPKI

Asad Haque

Executive Director of Security Architecture at Comcast

As the data in this year's report shows, the number of devices in connected homes is growing. Our customers now average 15 connected devices in their homes – up 25% since our report in 2020 – with our power users averaging as many as 34. What's even more interesting is the range of connected devices now available. Everyone thinks of the usual ones: computers, smart TVs, mobile phones, e-readers and smart doorbells and thermostats, but that list is quickly expanding. In looking at the connected devices protected by xFi Advanced Security, we're seeing new device categories like drones, cars, kitchen appliances, baby monitors, garage doors, robots and even pet accessories!

The proliferation of different types of connected devices has created a new challenge for consumers – how to securely integrate and manage all their devices, regardless of brand. That's where Matter comes in, an exciting new interoperability standard for the connected home. Just as the Bluetooth standard ensured short-range wireless devices from different brands worked seamlessly together, Matter is an industry-unifying standard that delivers reliable, secure connectivity so consumers can create connections between Matter-compatible devices across a range of brands. Initially conceived by Comcast, Amazon, Apple, Google and Samsung, Matter is now a global technology standard that recently released its initial "1.0" specification.

Because we were part of the very first discussions that led to the creation of Matter, we knew from the beginning that making it work in a secure manner was paramount, and that to achieve that we'd need a new way to identify and protect all of the individual devices in customers' homes.

Q: Why is Matter so important?

A: Since the disparate devices from different manufacturers and ecosystems in today's connected home can't really "talk" to each other, Matter was designed as a common "language" that all compatible IoT and smart home devices could use so consumers can control all their connected devices from the same place, regardless of brand, and then create advanced interactions between them. It's open source and leverages the existing WiFi and Thread protocols to run over local wireless networks in homes.

To do all that and ensure security, Matter needed to issue each device a digital certificate – it's called a DAC (Device Attestation Certificate) – but think of it like your driver's license or passport. It contains essential information, such as what the device is and what company made it, backed up with cryptographic proof so both Matter and the device connecting know the data is accurate. To ensure unique identities, every device needs its own DAC and given that there are already tens of billions of IoT devices out there the potential scale Matter requires is just massive.

Q: How did Comcast get involved with Matter?

A: Security at scale is something that Comcast knows how to do very, very well. Between the gateways, modems, Zigbee devices and other customer-facing and internal pieces of equipment on our network, we're responsible for securing close to 100 million devices. We were already involved in further enhancing the security of the Zigbee 3.0 specification (precursor to Matter) but recognized we needed a system to issue digital certificates to all the devices on our network to ensure digital identities and authenticity and make sure bad actors weren't pretending to be legitimate users to gain access to a device.

Since there was nothing commercially available on the market to address our needs, we created xPKI (Xfinity Public Key Infrastructure) as a scalable platform for Comcast to deliver millions of certificates daily to devices on our network. Although not part of the Matter 1.0 specification, we successfully integrated xPKI with blockchain to enable devices to make autonomous access decision based on microledgers without sacrificing performance. As of November 2022, we've deployed close to 300 million xPKI certificates to IoT devices and systems across the networks of Comcast and our partners.

And since Comcast was one of the founding companies involved with Matter, we realized Matter was trying to solve the same problem of issuing digital certificates on a massive scale – so we showed the very first Matter working group the device attestation (identification and authentication) we had already built based on xPKI. It was adopted and further refined by the Matter working group and then Comcast led the code contribution to enable it in the Matter software development kit (SDK).

Security at scale is something that Comcast knows how to do very, very well.

Q: Why are digital certificates so important to Matter and in connected homes?

A: A core tenant of cybersecurity is unique, immutable identities for devices that are imparted by digital certificates and associated private keys and secured within the device. For Matter, it was critical to build a strong cybersecurity foundation so customers feel at secure adding a Matter device on their home network.

This is such a big issue because previously many manufacturers would simply copy and paste the same digital certificate and private key on every device they shipped. This was unacceptable to Matter since without a unique digital certificate a network or system won't be able to distinguish between devices because they all present the same identity. Imagine the confusion if two individuals walked up to airport security with identical passports – even biological twins have different passports!

In fact, the airport analogy is a good example for how the system works. When we go to an airline desk, they check our identity from our license or passport (the DAC in Matter) and then issue us a boarding pass that allows us to get past the security checkpoint and board the flight listed on the boarding pass.

Similarly in Matter, once we authenticate an IoT device using its DAC, we issue it an "operational certificate" that is unique and separate from the original DAC and is essentially a "boarding pass" that allows the device to operate on our network. This is where scale is even more important because imagine millions of IoT devices waiting in queue to get their "boarding pass" so they can become operational on a customer's home network.

Trusted, verifiable and unique digital certificates using systems like xPKI's is the foundation in Matter for designing interoperable connected home solutions across multiple types of devices and different brands for a secure, reliable and seamless experience.

Q: Can you talk a bit more about how Matter will enable new connected home experiences?

A: This is the exciting part! Again, in today's connected home, consumers have a variety of smart devices that can control different things – opening a door, turning on a light, playing music and more. But each is individually controlled by the consumer through a different app or service.

Now with Matter – and the secure communications between uniquely identified devices based on their DAC – consumers can build individualized experiences spanning devices based on their personal preferences.

As an example, someone can set up the "get home from work" experience that is triggered when they open their WiFi-enabled garage door during the week. The garage door then communicates to other devices via Matter to turn on the kitchen and foyer lights, sets the temperature to 72 degrees and plays My Way by Frank Sinatra on the stereo. It's not The Jetsons quite yet, but it's a huge step forward for the smart home experience.

With a strong foundation in cybersecurity, Matter will continue to evolve and provide a secure and more immersive connected home experience for consumers worldwide as well as providing new opportunities for innovation for IoT device manufacturers, application developers, home broadband providers and retailers.

Security Never Sleeps

David White
Vice President, Security

Time is precious, and nowhere is this truer than in cybersecurity. The sooner an organization can identify a threat – whether it's a virus, or a hacker trying to break in – the faster it can respond, the better it can prevent real damage. Since we can't create a system that gives us more time, our technologists did the next best thing: building a platform that allows us to identify potential threats at lightning speed so we can respond and protect our systems, data, and customers.

Internally, we call this platform "Titan," which is fitting since it allows us to process a truly titanic volume of data in an unbelievably short amount of time, enabling us to act quickly to protect ourselves when threats emerge.

At its core, we designed Titan to dramatically reduce what cybersecurity experts call "mean time to detect" or MTTD.

First, a quick history lesson on why MTTD is a problem: Modern cybersecurity started after the commercialization of the internet. Back then – in the mid-1990s – companies were trying to keep troublemakers off their networks by using firewalls. These are systems that simply ask you for a password before letting you on the network. It separates a trusted network (your own) from an untrusted one to keep unauthorized people out.

But as the Internet evolved, so did the threats, and it quickly became apparent that firewalls alone were not enough to defend against the bad guys.

To keep pace with emerging threats, organizations added more-and-more security tools to their arsenal, each one designed to detect and stop a specific threat. There were intrusion detection/prevention systems, antispam, anti-phishing, antimalware, access management and more, each intended to thwart the specific types of threat.

This created a new problem: tool overload. ESG reports that the typical enterprise organization has 25-49 tools in their security infrastructure. Each of these tools "speaks" its own language when flagging threats, meaning that security personnel must check each tool to see if a threat is real or not (the latter being known as a "false positive"). And, since most alerts given off by tools are false positives (often when someone is doing something innocent – like logging on at an off hour), analysts waste a lot of time searching for a needle in a haystack.

It's a time-intensive process, making MTTD unacceptably high in most cases, and giving threat actors valuable time to cause damage. The most famous "dwell time" report is from Mandiant, which says the average attacker is on the network for 24 days before being detected. This number keeps going down, but it is still too high – a lot of damage can be done in an hour, never mind 24 days.

Enter Titan

With so many layers of protection deployed, Comcast is far from immune to the challenge of MTTD. With tens of millions of connected devices on the network, the amount of security data to review is huge, roughly 10 petabytes. But still, we saw an opportunity to significantly decrease MTTD across our networks based on a simple premise – if we could combine all our security infrastructure data in one secure location (known as a "data lake") and make it searchable, analysts would be able to correlate between tools, sync the data to create a coherent narrative and timeline of activity, and identify threats faster. Of course, easier said than done.

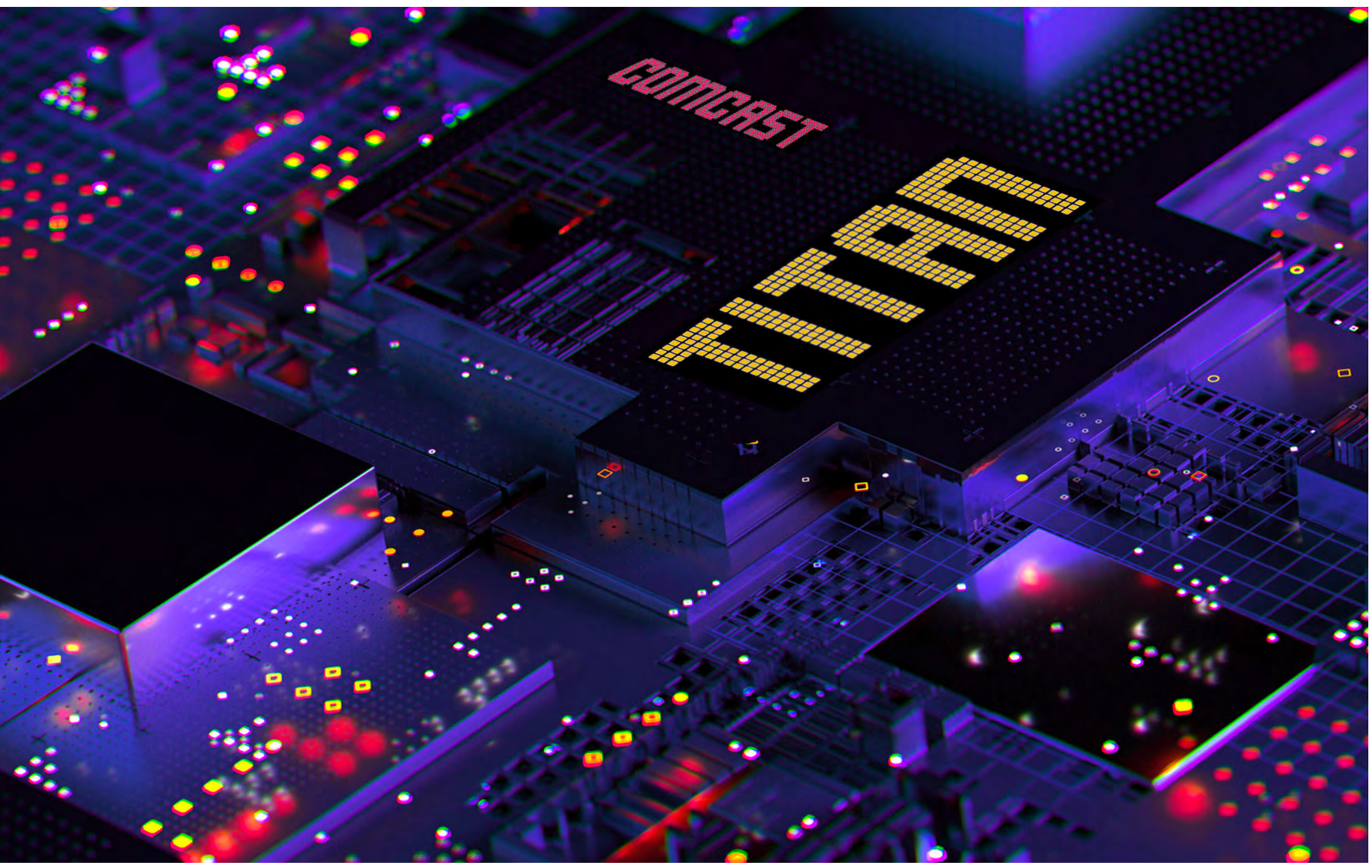
The solution became the threat intelligence platform we call Titan. The first, and most crucial, step in development was bringing all of our security information into a single location and normalizing and indexing that data to make it searchable. Customized data ingestors helped make this possible.

On top of this, we've built analytical models for various security risks or known threat vectors that we can constantly search against to identify and eliminate risks. These models include situations such as strange behavior for a Comcast partner logging into our network (e.g., they usually log in from New York but this access attempt is from Eastern Europe) or "living off the land" attacks where an intruder tries to get access to the network and then uses tools on it to infect more systems.

The Future Looks Bright

With our new innovations to ingest data from a range of security tools, normalize it to be consistent and run models against it, our threat intelligence platform truly advances the state-of-the-art cybersecurity for Comcast, our customers and the industry. When new threats, viruses or malware are announced, we can now identify indicators of compromise in as quickly as a few milliseconds.

And as with other Comcast innovations, we want to make this threat intelligence platform available to our partners to help bolster their cybersecurity efforts. In the meantime, Comcast customers can rest assured that we are on the leading edge of security, protecting their connected homes and personal data at all times.



Our threat intelligence platform truly advances the state-of-the-art cybersecurity for Comcast, our customers and the industry.

Your Data Privacy is Our Top Priority

Bahman Rashidi,

Ph.D., Director, Cybersecurity & Privacy Engineering Research

Data breaches have become a part of daily life. We hear about a breach on the news and hope we don't get the dreaded email saying our data was compromised. But while data breaches may seem sadly normal, we don't think they have to be, and we're committed to helping prevent them, not just at Comcast, but everywhere.

This is why my entire team wakes up every day. We research and build technologies that either strengthen our existing systems and processes or create entirely new cybersecurity capabilities – all to protect our customers from potential data breaches.

Most importantly, our focus is always on how to proactively prevent any private information from getting out in the first place. And this is something that is a bigger challenge as software, applications and systems are increasingly developed outside the boundaries of enterprises on cloud-based platforms in collaboration with other developers and open source communities.

One of those public platforms is GitHub, the largest open source community on the internet with millions of code and software repositories and users. Like most other R&D companies, Comcast development teams working on our customer-facing applications as well as our own internal systems use GitHub every day – whether it is publishing code, collaborating on software development or using code from GitHub for new projects and solutions.

However, with so much information being uploaded every day, GitHub also presents a unique cybersecurity challenge.

Comcast Gets Proactive on Data Privacy

xGitGuardTM is software built by Comcast engineers to keep authentication secrets, including passwords as well as API tokens and keys (essentially ways to ensure a user or application is legitimate), from inadvertently being uploaded to open source repositories on GitHub. As software developers are piecing together different code for an application, there can sometimes be sensitive or private information within the code that could be missed before it gets uploaded to GitHub.

xGitGuard prevents this from happening by detecting this type of information before it is uploaded. To detect sensitive information and protect data privacy, xGitGuard uses advanced natural language processing and a unique six-step process:

01

Search

using a two-step search process, xGitGuard searches all of GitHub, but only returns results for documents that are relevant and with sensitive info.

02

Filter

a scalable and intelligent filter ability so only documents that have not already been reviewed and processed are returned.

03

Detect and Extract Secrets

using artificial intelligence, xGitGuard is able to drill into documents and remove any sensitive information.

04

Developer ID

the software is then able to identify the developer (and associated company) who posted the code on GitHub for notification.

05

Validate Secrets

xGitGuard uses a special model trained with historical detection data to ensure the information extracted is, in fact, secret.

06

Submit for Remediation

any secret information that has been validated is then submitted for remediation to various engineering teams.

More importantly is how Comcast uses xGitGuard. Code from engineering teams is now automatically scanned using the tool before it gets posted on GitHub, to ensure there is no private information in it. In addition, xGitGuard also scans all of GitHub daily looking for private information. For Comcast, it allows our engineering teams to take advantage of the full technical benefit of GitHub while also maintaining peace of mind that their work isn't inadvertently opening the door for privacy issues.

Open Sourcing xGitGuard to Help the Industry

We also recognized this is a wider industry issue, which is why we open-sourced xGitGuard earlier this year. The idea was to give other companies the ability to protect sensitive information and empower the open source community to enhance and expand the software for everyone's benefit.

As with many other Comcast innovations, xGitGuard came out of necessity. As the team looked for a solution, it realized that the existing open source and commercial tools could not effectively handle GitHub's scale and only were able to find secrets that fit to a specific data pattern. In short, they were ineffective for Comcast's purposes, so the team built xGitGuard, but realized it would benefit both Comcast and the broader industry.

And, since launching it last March, we've made significant improvements to the core modeling engine to improve the detection capabilities with more context into what is actually sensitive and needs to be deleted. In addition, we've heard from multiple researchers and developers at other companies with suggestions on improvements to xGitGuard as well as ways we could even collaborate together to improve data privacy for the industry.

As we continue to work on xGitGuard with the open source community, we're already working on other innovations to ensure our customers' privacy. Some of these include working on new threat modeling as part of our application development process that looks at it from the perspective of a cybercriminal, to find vulnerabilities and weaknesses they would want to exploit and address them in advance.

And, recognizing that no two of our customers are the same, we're also looking to customize our privacy tools by creating a variety of "privacy personas" and building the necessary security for them as we design software. So, maybe an individual in a city apartment is interacting with Xfinity Internet and X1, but a family in the suburbs has a connected home with 20 different devices. We want to understand how each user is interacting with our network and services, and the risks associated, so we address those in the software design and development stage to provide more customized data privacy protection.

Data privacy is a huge issue for the industry and the root cause of many data breaches, which is why it's such a big deal at Comcast. xGitGuard and the other technologies our cybersecurity and privacy engineering teams work on every day highlight how we are innovating new data privacy solutions that start protecting our users – from the original application design stage through to actual coding and development – well before the software is launched and consumers start using it.

5 Tips for Securing Your Connected Home From Cyber Threats

The global pandemic forced people of all ages to become more reliant than ever on the internet. And, as the necessity for digitization grew in both our personal and professional lives, the number of connected devices worldwide soared with it. Comcast estimates that the average home on its network has 15 such devices now and power users have upwards of 34 – from laptops and gaming consoles, to smart TVs and even connected cars and baby gear.

The digital world we're living in provides many benefits, but it also has expanded our personal security "footprints" to encompass every connected device in the household – even those without screens – and protecting them can seem overwhelming.

The good news is, there are simple steps that anyone can take to help prevent bad actors from infiltrating your connected home. Here are five best practices that will put you on the path to protecting your home, yourself and your family.

01

Create Strong, Unique Passwords

Weak and "repeat" passwords continue to be driving causes of network and device breaches. Though you may be tempted to create simple passwords that you can remember, we cannot overstate the importance of generating complex, unique passwords for the different services and websites you use. Avoid using generic passwords that are easy for hackers to guess (e.g., "qwerty12345") as well as passwords derived from personal information that is easily searchable on social media (e.g., your name, your pet's name, your birth date, your favorite sports teams, the city you were born, etc.). The strongest passwords are long and use a combination of letters, numbers and special characters. Passphrases – passwords made up of a phrase or sentence (e.g., Penguins are the cutest animals at the zoo) – are a great way to enhance password security. Good password hygiene is especially important for the password you use to protect your home network. Use a strong, unique password that cannot be easily guessed. And, change your passwords on a regular basis, so any compromised credentials will be rendered useless.

Use a strong, unique password that cannot easily be guessed.

- Penguinsarethecutest
- qwerty12345

02

Use Multi-Factor Authentication

Multi-factor authentication (MFA) takes account and device security one step further by requiring you to confirm your identity using two or three different factors — typically, something you know (e.g., a password or challenge question), something you have (e.g., a unique, time-sensitive code sent to your mobile phone or email), or something you are (e.g., a fingerprint or facial recognition). Always enable MFA if it's available, as it can provide an added layer of protection that makes it that much harder for bad actors to penetrate your digital life.

03

Enable Auto Updates on Devices

The “system update required” messages on our devices always seem to come at the worst possible times — when we’re in the middle of a big work assignment, trying to help our kids with online schoolwork, paying bills, etc. And, it can be easy to leave these notifications for another day. But, firmware and system updates provide more than just product enhancements — often, they include new security features or patches that are essential to maintaining device and network security. Because of this, it’s important to run system updates on all connected devices — from laptops and mobile phones, to smart thermostats and voice assistants, and everything in between — as soon as the notifications come in. This is especially critical for smartphones that regularly have system updates and security patches that users often delay installing. According to data from Mixpanel, only 41% of iPhone users are on the new iOS 16 while 51% are on iOS 15 and 8% on an even older version. Many devices have an “auto update” setting. Enabling “auto update” it on all new and existing devices is an easy and pain-free way to ensure you always have the latest security updates and firmware running.

41%

Only 41% of iPhone users are on the new iOS 16.

04

Take Inventory of Your Connected Devices

Xfinity households have 15 connected devices, on average, with power users averaging as many as 34. These high numbers can make it difficult for us to keep track of our device inventory. And, it’s likely that, as new devices are purchased and connected to home networks, old ones are neglected. But just because we’re not using these devices regularly, doesn’t mean they aren’t posing a threat to our security. We’re starting to hear about the “Internet of Forgotten Things” — those devices that we don’t remember we have but that are still connected to the network and introducing security risks — and it’s a problem that isn’t going away anytime soon. To prevent this in your home, it's good to periodically take an inventory of all your your devices. An easy way to check is through your internet provider’s apps and tools. For example, the Xfinity app shows you a list of all the devices currently connected in your home. Once you’ve identified devices you no longer use, and then erase any personal information from those you no longer use and recycle them.

34

Xfinity households have 15 connected devices, on average, with power users averaging as many as 34.

05

Educate Yourself on Phishing

Cybercriminals have become increasingly adept at crafting phishing emails, a.k.a. fraudulent emails impersonating legitimate people (e.g., a family member or friend) and organizations (e.g., a bank or school) to trick the reader into divulging personal or financial information. Senders of phishing emails typically ask recipients to click a link or open an attachment within the email, tricking them into downloading malware onto their connected devices – which then opens a gateway to their home networks. While phishing emails can be very convincing, there are some common ways to detect when something is amiss. Tell-tale signs of phishing include spelling errors in the subject line or email body, suspicious links or attachments within the email, tones of misplaced urgency, unfamiliar senders, or slightly misspelled company names in the sender’s email address. If you have any doubts, reach out to the family, friend or organization the email is from to inquire about its legitimacy.

Secure Your Internet-Connected Devices at Home

Connected devices have transformed the way we live, play and work, but to continue experiencing their incredible benefits without the associated risks, we need to keep them secure — and this requires multiple layers of protection. In addition to following the best practices above, it's also a good idea to check in with your internet service provider to see what security solutions they offer for their home gateways. For example, Comcast's xFi Advanced Security service protects nearly 54 million home users and can add safe browsing and data protection on-the-go through xFi Complete. With the right tools and security habits, you can help protect your connected home and everyone within it.

COMCAST

CORPORATE.COMCAST.COM