COMCAST

2020 Xfinity Cyber Health Report

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

03 A NEW CHALLENGE: A WORD FROM OUR CHIEF PRODUCT AND INFORMATION SECURITY OFFICER

05 XFINITY CYBER HEALTH REPORT

07 SURVEY RESULTS ON CONNECTED HOME SECURITY

12 HOW ARTIFICIAL INTELLIGENCE IS PROTECTING CONNECTED HOMES

14 Q&A WITH A COMCAST SECURITY EXPERT

18 5 TIPS FOR SECURING YOUR CONNECTED HOME

A NEW CHALLENGE: SECURING TODAY'S CONNECTED HOME

You've probably accumulated quite a few connected devices over the years. It started with PCs and laptops, and then moved to smartphones, gaming consoles and printers, and now you're adding security cameras, voice assistants, smart thermostats and, believe it or not, even smart toasters! Cisco projects the average home will have 13.6 networked devices by 2022.[1] Welcome to the "connected home."

When the COVID-19 pandemic started, many of us experienced how our connected homes have digitized almost every aspect of our world. We couldn't send our kids to school or go to the office (not to mention movie theaters, restaurants, exercise classes, or even the doctor's office), but connected devices digitized those experiences so we could carry on with our lives. Mom would be in one room doing a video conference while her daughter would be in another room taking an online algebra class, and her son was ordering a pizza delivery using a smart speaker.

What many people don't realize is that connected devices can also pose a security risk. Cyber criminals target them because many have little or no security protections (unlike your laptop), they are often left unattended and some of them don't even have screens — which means they can be more easily hacked without you even knowing it.

Bad actors attacking your connected devices could be trying to spy on your household through a camera, or to add the computing power of one of

13.6

CONNECTED DEVICES PER HOUSEHOLD BY 2022

[1] *"Cisco Annual Internet Report (2018–2023) White Paper," Cisco, March 2020*

your devices to their army of co-opted computers (called "botnets"), or even to use a connected device as an "on-ramp" onto your home network, where they could potentially attack other devices and steal your identity information to commit fraud.

The risk to connected homes is expanding: 61% of consumers plan to buy at least one connected-home device this holiday season, according to our survey for this report. In my role as Chief Product and Information Security Officer at Comcast, I have all-too-clear an understanding of how pervasive these threats are and why it is so critical to block them proactively. Our xFi Advanced Security service blocked 6 billion cybersecurity threats in our customers' homes between January and August this year, or **about 104 cyberthreats per household each month**. And during the early part of the pandemic, threats increased 12% as hackers looked to take advantage of the increase in online activity in connected homes.

These threats ranged from phishing attacks designed to fool you into clicking on malicious links in emails, to websites attempting to download malware onto your computer, to hackers trying to break into your connected home devices so they can gain entry onto your network and access personal information.

To gain a better understanding of today's connected homes and the behaviors of the people living in them, Comcast created the Xfinity Cyber Health Report. This is the first report of its kind, combining data from millions of connected Xfinity xFi homes across the country, with a comprehensive survey on the habits and beliefs of the people living in those homes. In the following pages, you can see how your connected home stacks up against others, determine how secure your digital world really is, and get some tips and recommendations on how to better protect everything in your connected home – from devices and people, to all your data.

I hope you find this report helpful, and please know that we are working, 24x7, to assist you in making your connected home safe from cyber intruders.

104

CYBERTHREATS ON AVERAGE PER HOUSEHOLD EACH MONTH

6B

CYBERSECURITY THREATS BLOCKED IN OUR CUSTOMERS' HOMES BETWEEN JAN. AND AUG.

12%

INCREASE IN THREATS DURING THE EARLY PART OF THE PANDEMIC

Sincerely,

NOOPUR DAVIS
Chief Product and Information Security Officer, Comcast

xfinity xFi

2020 XFINITY CYBER HEALTH REPORT

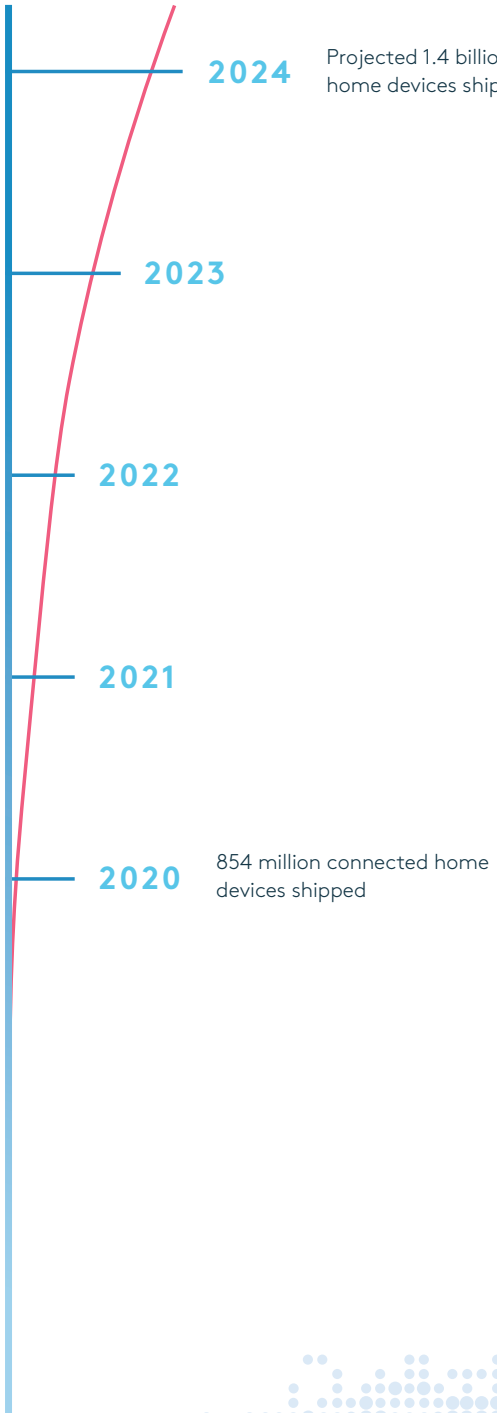
THE CONNECTED HOME IS NOW A REALITY

For this report, we've summarized the threats targeting our customers and the devices in their connected homes. The report provides the industry's first view — on a massive scale — into these threats to consumers. The situation is clear: **The connected home leaves us vulnerable to cyberthreats.**

The "connected home" is now a reality. International Data Corp. estimates 854 million connected-home devices will be shipped by manufacturers in 2020, and that number is projected to grow to nearly 1.4 billion by 2024. [2] Video entertainment is the largest category of connected-home devices, followed by home monitoring/security devices and smart speakers.

Unfortunately, these devices also bring risk into the home. These risks include bad actors hacking into connected devices and using them as an on-ramp onto the home network, so they can search for and steal valuable data and identity information. Or, these bad actors 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. with 27 million Internet customer households, Comcast sees this happen every day. That's why in January 2020, we launched xFi Advanced Security as a free service to all of our Internet customers with the xFi Gateway. Since that time, we've been able to detect and block 6 billion threats to protect our customers.



[2] *"Worldwide Quarterly Smarthome Tracker," International Data Corp, September 2020*

BREAKDOWN OF OBSERVED CYBERSECURITY THREATS IN THE HOME

COMMON TYPES OF CYBER ATTACKS

Just what are bad actors trying to do to your connected home? First, let's take a look at the most common security incidents seen by xFi Advanced Security:

01
Unsafe Browsing: This happens when a website tries to download malware or other bad content onto your device.

02
Unauthorized Access: This is when hackers attempt to fraudulently log into your connected devices.

03
Distributed Denial of Service: Bad actors launch large streams of network traffic from "botnets" to overwhelm networks and systems, often as part of blackmail schemes. Compromised connected-home devices can be made part of these malicious botnets.

04
Suspicious Device Activity: When devices are hacked, they will behave strangely – communicating back to hackers, etc. When xFi Advanced Security detects strange behavior, the customer is notified so they can take care of the problem.

COMMONLY TARGETED DEVICES

01
Computers and Laptops: The richest targets in the home due to all of the valuable data they hold, but also the best protected.

02
Smart Phones: Similar to computers and laptops.

03
Networked Cameras: Often not very secure, and can be used for eavesdropping or incorporation into botnets.

04
Networked storage devices: Often contain valuable data and are unattended for long periods of time, which can mean security protection is out of date.

05
Streaming video devices: Hackers often attack these to get log-in credentials and credit card information.

SURVEY RESULTS ON CONNECTED HOME SECURITY

CYBER THREATS IN THE CONNECTED HOME: CONSUMER CONCERNS AND PRACTICES

Many people – 95 percent – don't realize the extent to which their connected homes are under attack, as outlined in our xFi Advanced Security data. To gain a better understanding of consumer opinions and practices around connected-home security, Comcast commissioned Wakefield, a market research firm, to conduct a survey of 1,000 nationally representative adults ages 18 and older in September 2020. The following pages show the results of that survey, and what it means to the connected-home future.

95%

OF SURVEY RESPONDENTS GROSSLY UNDERESTIMATED THE VOLUME OF ATTACKS THEY FACE EACH MONTH

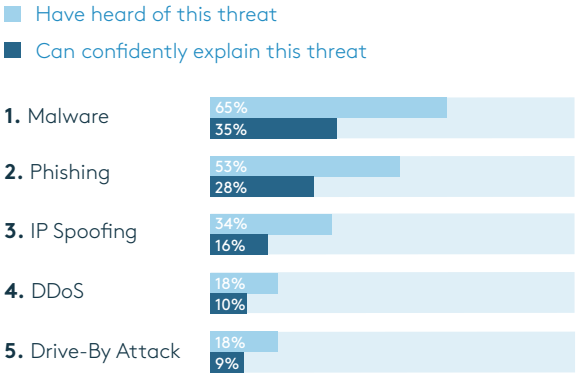
UNDERSTANDING SECURITY THREATS

The survey initially sought to establish people's level of knowledge about various types of cyber threats. There was a gap between people's general awareness of threats, and their actual understanding of how those threats work. For example, 53% had heard of phishing, but only 28% believed they could confidently explain what phishing is. This gap was consistent across all categories, as can be seen in Figure 1.

Respondents also were not aware of the large volume of threats targeting their home networks.

CONSUMER KNOWLEDGE OF COMMON CYBER THREATS

FIG 1



20%

HAVE NOT HEARD OF ANY OF THESE

42%

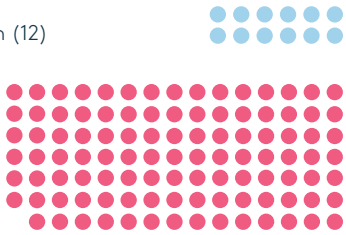
COULD NOT CONFIDENTLY EXPLAIN ANY OF THESE

CYBERTHREAT MISCONCEPTIONS IN THE HOME

FIG 2

2.1 Perceived Amount of Cyber Threats per Month (12)

2.2 Actual Amount of Cyber Threats per Month (104)



WHEN ASKED A SERIES OF SEVEN "TRUE OR FALSE" QUESTIONS ABOUT BASIC CYBERSECURITY ISSUES

FIG 3

96% of respondents could not accurately answer 6 basic cyberthreat questions correctly.

42% of respondents answered three or more incorrectly – which would be a failing grade in school!

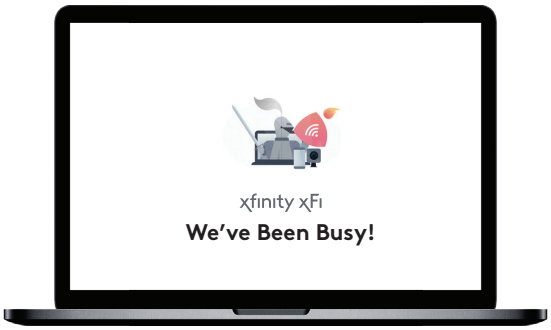
IMPACT OF COVID-19 ON CONSUMER CYBER-BEHAVIOR

With some schools and offices closed during the COVID-19 pandemic, it's not surprising that people are relying on their home Internet connection more than ever. **86% of respondents agreed they rely more on their Internet connection than before the pandemic.**

With the pandemic causing home Internet connectivity to become more critical than ever for work and school – not to mention entertainment, ordering food and even virtual doctor visits – most survey respondents also became more concerned about cybersecurity.

PERCEPTION AND REALITY ARE NOT IN SYNC

The survey showed a disconnect between perception and reality when it comes to cyber-safe behavior. **A large majority (85%) of respondents indicated they are taking all the necessary security precautions needed to protect their home networks. And yet, a clear majority of respondents (64%) admitted to behaviors that open themselves up to attack.** For example, reusing passwords enables attackers to gain access to multiple personal accounts with a single stolen password, and sharing passwords increases the likelihood they can be stolen in the first place.



4 in 5

OR 83% OF RESPONDENTS WOULDN'T KNOW IF THEIR NON-SCREEN DEVICES HAD BEEN HACKED

85% OF RESPONDENTS SAY THEY ARE TAKING NECESSARY SECURITY PRECAUTIONS

64% ADMIT TO BEHAVIORS THAT OPEN THEMSELVES UP TO CYBER ATTACKS

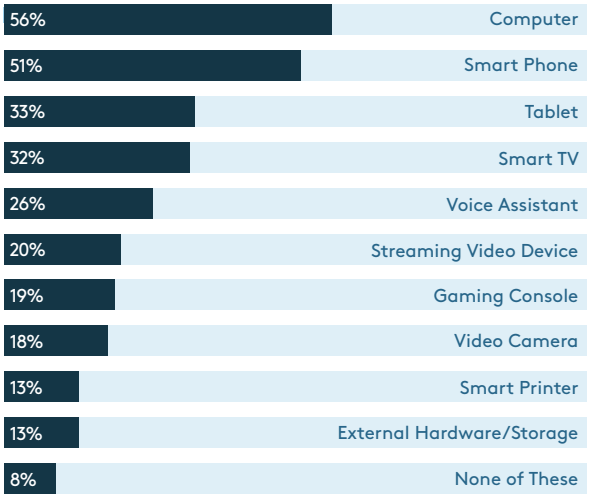
CONSUMERS ARE DISCONNECTED FROM REALITY WHEN IT COMES TO CYBER THREATS

There was also a disconnect between respondent perception and reality about which of the devices in their home were most likely to give cyber criminals access to their home network. Earlier in this report, we showed the connected devices most targeted, based on real-world data from xFi Advanced Security.

Our survey, however, shows **people underestimate the risk associated with cameras, and networked-storage and streaming video devices. Figure 4 spells out this disparity.**

FIG 4

WHAT CONSUMERS THINK IS MOST TARGETED IN THE HOME



DEVICES THAT ARE ACTUALLY TARGETED

1. Computers & Laptops

2. Smart Phones & Tablets

3. Networked Cameras

4. Networked Storage Devices

5. Streaming Video Devices

And, the connected-home environment will continue to expand. Our Xfinity xFi users have an average of 12 devices per household and added on average two devices over the past year, but some high-end users have as many as 33 devices and added five since last year. This trend is echoed in our survey as **61% of respondents plan to buy at least one connected device during the upcoming holiday shopping season.**

But, connected-home devices are not like PCs — you can't run commercial off-the-shelf security software on them, and in many cases people forget about them after they're installed. This makes them more vulnerable to potential compromise because firmware won't be updated and, as "unattended" devices, people won't notice if they've been compromised. And yet, 65% of respondents indicated that they feel confident that most connected home devices are protected from most cyberthreats.

The good news is, 93% indicated security is at least somewhat important to their purchasing decisions. Figure 5 shows security does command the attention of most people in connected homes.

XFINITY XFI USERS HAVE AN AVERAGE OF

12

DEVICES

SOME USERS HAVE AS MANY AS

33

DEVICES

61%

OF RESPONDENTS PLAN TO BUY ANOTHER DEVICE THIS HOLIDAY SEASON

FIG 5

LEVEL OF IMPORTANCE RESPONDENTS PLACED ON BUILT-IN SECURITY OPTIONS FOR THEIR DEVICES

HOW CAN CONSUMERS PROTECT THEMSELVES?

It's not realistic for consumers to become cybersecurity experts — so it's not surprising to see gaps between what people think they are facing with cybersecurity attacks, and what they are actually facing. And, there is also a general lack of understanding around how to secure the connected home. **53% of consumers indicated they either don't know if their Internet service providers offer protection against cyberthreats, or that their providers don't offer such protection.**

The absence of awareness about potential solutions is a problem, because Internet service providers can help protect the connected home since their "gateway" is between the Internet and the home network. The next section takes a look at how xFi Advanced Security does exactly that for our customers using Xfinity xFi Gateways.

HOW DOES XFI ADVANCED SECURITY PROTECT WIFI CONNECTED DEVICES IN THE HOME?

MONITOR

Monitoring is extended to any device that is connected to the home network wirelessly.

BLOCK

Xfinity AI and machine learning monitor and analyze WiFi traffic, and automatically block suspicious activity.

INFORM

Customers can review a list of digital security-related actions that were taken each day.

HOW ARTIFICIAL INTELLIGENCE IS PROTECTING CONNECTED HOMES

SANTERI KANGAS
CTO of CUJO AI

Historically, cybersecurity protection was one step behind bad actors. Hackers would devise a way to exploit a piece of consumer technology, usually to steal data. Technology makers would then push out a "patch" to all their customers to address the issue and protect customers. Unfortunately, this reactive approach doesn't help people who have already been victimized by an attack. And, as soon as hackers realize their original method of attack no longer works, they would find new vulnerabilities, and set off a new cycle of exfiltration and patching all over again.

When we developed the technology behind CUJO AI, we wanted to break this cycle and be one step ahead of the attackers. To do this, we created a continuous "learning" system that employs its cumulative knowledge to recognize and prevent attacks before damage can be done. It's similar to how, in the real world, if you see a person walking into a bank wearing a Halloween mask and carrying an empty bag, you would probably notify someone of a potential bank robber.

How can you create a system that can do this kind of thinking? Through artificial intelligence (AI). By using AI, security systems can "learn" what's normal and what isn't for devices on a network — and then use that information in the digital equivalent of blocking the person wearing the Halloween mask from entering the bank. Until now, this kind of technology was only available in high-end security systems used in large corporations. In a revolutionary step forward for consumer cybersecurity, Comcast partnered with CUJO AI to provide this capability to its customers on a massive scale through xFi Advanced Security.

The paramount reason for taking this step was to protect the wide array of smart devices in the connected home – from doorbell cameras to network storage devices, streaming video players, printers, and smart appliances. And while all of these connected devices have made our lives more productive, automated and enjoyable, they bring new risks. Most people install these devices and forget about them – especially when it comes to updating their firmware or installing software patches. This leaves a lot of "open windows of opportunity" in connected homes for hackers to exploit.

And we know their playbook. These hackers run massive scans across the Internet to identify networks and devices with vulnerabilities and then exploit them with scary-sounding malware like "IoT Reaper" and "Gafgyt." Once a connected-home device is compromised, the malware typically scans other home network devices to spread a virus. From there, the hacker can look for sensitive

CUJOAI

WHAT IS CUJO AI?

CUJO AI is the global leader in the development and application of artificial intelligence to improve the security, control and privacy of connected devices in homes and businesses.

data or use the compromised machines as part of a "botnet" to attack a larger target, such as a corporation, government agency, or large retailer.

This is why we built CUJO AI to run in the cloud and protect each connected home by analyzing and blocking threats in real-time at a customer's broadband gateway before the traffic enters the home. We have more than 750 million devices under protection, which gives us a lot of data to learn from so we can understand how those devices are supposed to act under normal circumstances.

By using AI, security systems can "learn" what's normal and what isn't for devices on a network – and then use that information in the digital equivalent of blocking the person wearing the Halloween mask from entering the bank.

For example, suppose a customer installs a specific smart thermostat or video doorbell. In that case, our system recognizes the vendor, model number, software version it is running and its expected network traffic – such as sending information to specific servers in California at a certain time each day. If that device starts acting abnormally – sending traffic to new locations or at different times of day – then we can block it, analyze it and notify the customer it was addressed.

Even for brand new devices, it only takes about 24 hours for our system to analyze, understand, and profile them for monitoring going forward. So, with each device added, CUJO AI's "brain" gets that much smarter about how to protect your connected home.

Getting the benefit of this AI technology is easy for Comcast customers – simply download and log into the Xfinity app to activate xFi Advanced Security for free. Once that's done, malicious traffic is stopped at your "digital front door" — your xFi Gateway — and your connected home will do exactly what it's supposed to do: make your life better.

Q&A: DESIGNING PRODUCTS AND BUILDING A CULTURE FOCUSED ON CYBERSECURITY

LARRY MACCHERONE
Comcast Cyber Security Expert

Is your smart thermostat currently on the front lines of a "botnet" army trying to infiltrate a company's computer systems in Europe? Or maybe that inexpensive webcam you bought to keep an eye on your dog while at work is actually giving a hacker halfway around the world a view into your home?

While everyone knows the importance of keeping their information and identity secure, it gets confusing for some people when faced with unfamiliar terms like malware, phishing, IP spoofing, drive-by attacks and distributed denial of service. This is reflected in our 2020 Xfinity Cyber Health Report: Among the respondents in our survey who have heard of cyber threats like these, 42% are unable to confidently explain them to someone else and 28% believe no cyber threats hit their home network each month.

As the number of devices in our homes grows, the "attack surface" — the range of opportunities and methods by which hackers could gain access to our identity and data — increases and leaves consumers wondering what is the best approach for protecting their connected homes.

To help provide some answers, we sat down with Larry Maccherone, a Distinguished Engineer in Comcast's Security and Privacy group. A software engineer, entrepreneur and data scientist, Larry is an industry-recognized thought leader in security and privacy issues.

As a simple test, ask yourself, "Have I updated the firmware on all my connected devices recently...or ever?" That firmware often fixes security holes, so if the answer is "no," you have devices in your home open to compromise.

Why is securing the connected home so challenging?

In large part, the main issue is that cybersecurity is often viewed as a separate product that a consumer buys and bolts on to something else. Years ago this was pretty straightforward — you bought a laptop and then bought anti-virus software to protect that specific device. As long as you kept the anti-virus updated, you had some protection.

Today, our homes have an average of 12 connected devices in them. Some of these devices have screens, including laptops, tablets and smartphones; while others are unattended or don't have screens and are harder to monitor and protect — these include smart thermostats, voice assistants and cameras. As a simple test, ask yourself, "Have I updated the firmware on all my connected devices recently... or ever?" One of the most common reasons for a firmware update is to plug security holes, so if the answer to the prior question is "no," you probably have devices in your home open to compromise. But, even if the answer is "yes," devices may still have security holes that the manufacturer has not yet found, so they are still open to compromise.

How is the industry responding to this challenge?

I think the biggest change has been the trend to build security into products and services from the beginning of their development, rather than "bolting on" security after the fact. This removes confusion and complexity for consumers and automatically adds more layers of protection, which is critical.

Think of credit card companies that now monitor accounts and call customers when there is a charge that deviates from your normal behavior. For example, maybe a person typically just charges a few hundred dollars per month in the Philadelphia area and suddenly there is a $10,000 charge at a store in Canada. Years ago, that person would have to review their bill, identify the fraudulent charge, and then call the credit card company. Today, that same person's account is closely monitored and they receive a timely, proactive text or app notification flagging the potential for a fraudulent charge.

How does security get infused into broadband services?

In the technology industry, cybersecurity was once exclusively handled by a totally separate team from those developing products and services. In this old model, the engineering teams just focused on building the product or service and then threw it over the fence to the cybersecurity team to let them worry about securing it. With this approach, the product engineers aren't thinking about security as they design and build a product, and the cybersecurity team is forced into figuring out how to implement security after the fact. This friction between the team designing products and those securing them creates a problem — it's like building a car with no safety features, having it roll off the assembly line, and then having safety engineers figure out how to retrofit the car with airbags and seatbelts.

At Comcast and throughout the technology industry, we've been on a multi-year path to fundamentally change how we build secure products. One of the ways we do that is through a product design model called "DevSecOps," which is a technical way of saying that the teams of software developers, designers and engineers who build our products, are also playing a much bigger part in securing those products. This approach results in simpler and stronger security for broadband services.

How does Comcast approach cybersecurity from a development perspective?

While we are the nation's largest broadband provider with 27 million Internet subscribers, you can also think of Comcast as a technology company. We have more than 10,000 developers spread across 500 product teams building everything from the xFi Advanced Security service and xFi pods, to Xfinity X1 and Flex. Every day these teams are releasing new features and capabilities to make our products and services more secure, reliable and valuable to our customers.

We found that the friction between the product and security teams I mentioned earlier was slowing down our development. When I joined a few years ago, we decided to change the culture completely and empower developers with the training and development framework to build security in from the beginning. It's a philosophy we call, "Security by Design."

How does "Security by Design" benefit Xfinity customers?

Rather than have separate engineering and security teams as I mentioned earlier, we've created a culture where they work together as a single team creating inherently secure products and services. This means our customers' broadband connections — along with all connected devices in the home and the various other apps and services we provide — are continuously updated, improved and enhanced to automatically protect our customers' identities, privacy and data.

So, now our customers can go in the Xfinity app and see all the threats we've proactively blocked from entering their connected homes — because when security is "baked in," it's that easy to see how you're protected.

Just one xFi Pod paired with your xFi Gateway is recommended to elevate the WiFi experience for most households. Since March, demand for xFi Pods has doubled as customers continue to join meetings, virtual classrooms and online social events from home.

TOP 5 TIPS: SECURING YOUR CONNECTED HOME FROM CYBER THREATS

PATTI LOYACK
Vice President of Connectivity Services, Comcast

For consumers, the volume and complexity of cyber threats can seem overwhelming, especially given how many devices we have in our connected homes today.

Keeping the bad actors out of your devices and off your network does not have to be overwhelming — in fact, all it takes is a few simple practices. Just as you protect your physical home with a variety of security "layers" — locks, lights on timers, exterior lights with motion sensors, alarms and other things — you can similarly protect your virtual home network and the devices connected to it.

Here are some of our key tips on easy ways to do that.

01. USE MULTIFACTOR AUTHENTICATION

If available, *always* enable multifactor authentication, which allows websites or services to confirm your identity using a combination of two or three different factors – typically something you know (a password or challenge question), something you have (a unique, time-sensitive code sent to your mobile phone) or something you are (a fingerprint or facial recognition on your phone). While it adds an extra step to logging in, it's a simple and easy way to protect your accounts and information.

02. ENABLE AUTO UPDATES ON DEVICES

Since our smartphones are essentially an extension of ourselves at this point and we use our laptops or tablets each day, we are a lot better about responding to "system update" notifications right away. But when was the last time you did a firmware update on your smart thermostat, printer, webcam or voice assistant? Those updates often add new security features or patch holes, so they are critical to maintaining security. Most devices these days have a setting to enable "auto updates," so they always have the latest firmware. Enable that setting whenever you set up a new device.

03. THINK BEFORE YOU CLICK ON THAT LINK

Hackers have become increasingly sophisticated in the design, layout and content of phishing emails or sites infected with malware. Often people receive an email that seems to be from their bank, school, friend or family member, or other authority with some urgent need for their information. The emails can be very convincing. Here are three simple questions you can ask yourself to screen an email:

01 Look carefully at emails that are not a direct response to something you requested – do you recognize the sender's email address?

02 Have you made an inquiry related to this email recently? If so, does the sender's email address match the source you were expecting to respond to your request?

03 Is there false urgency in the email? Do you really not have time to call the person requesting you to send money urgently?

Take a minute, review the email and be on guard for irregularities. If you have any suspicions, trust your instincts. You may want to delete the email or reach out directly to the company to inquire about its legitimacy. Never click on unknown or suspicious links!

04. BROADBAND CONNECTION SECURITY

Just like you have a strong lock on your front door, for a hacker to get into your connected home, they need to come through its digital equivalent: the gateway device of your broadband connection. 53% of respondents in our survey said their Internet service provider (ISP) was not protecting their home network or they weren't sure. Talk to your ISP and see what security they offer for their broadband gateways. For example, Comcast Internet customers with an xFi Gateway can simply log into the Xfinity app and they are automatically protected by xFi Advanced Security, providing a proactive barrier between their connected home and the "Wild West" of the Internet.

05. STRONG PASSWORDS

Make sure to create distinct passwords for different services and websites you use. They should be hard for a hacker to guess if they are trying to use your public information (your name, address, etc.) or what you post on social media (names of pets or children, favorite sports teams, high school or college mascot, etc.). Always avoid generic passwords that are easy to guess ("1234abcd" or "p@ssw0rd") and keep in mind that a long, simple, easy-to-remember phrase is a better password than a short, complex one. You should always use unique passwords for sensitive sites like banking or investing, and even services like Netflix or Amazon that may store your personal and credit card information. Also, do not share passwords with friends or family, since this puts them outside of your control and exposes you to more risk. It's also good practice to change your passwords on a regular basis. Using a password management app can be a good way to easily manage a large number of different, unique passwords.

1234abcd

$box#bottle%9

"Always avoid generic passwords that are easy to guess ("1234abcd" or "p@ssw0rd")" . . . You should always use unique passwords for sensitive sites like banking or investing, and even services like Netflix or Amazon that may store your personal and credit card information."

From working at home, studying remotely and telemedicine check-ups, to streaming the latest Hollywood blockbusters and video calls with far-away relatives, connected homes are changing how we live, work and play — all at home in this "new normal." Feel confident that you can do it securely by taking the steps we outlined and adding multiple layers of security to protect your connected home.


COMCAST