F-Secure®

# Staying ahead of cyber threats in the age of AI

# Contents

1

# Welcome to the future: An introduction to the AI revolution, by Mikko Hyppönen

I first heard about artificial intelligence when I was 13 years old.

As I was reading Tekniikan Maailma, Finland's popular science magazine, I came across a compelling eight-page story about the incredible growth of computing power. The article speculated that one day in the future we might have enough processing capability and storage capacity to build machine learning frameworks that would be smarter than humans. This was 1983.

Predictions are hard, and it's not surprising that this story got one thing wrong. It suggested we'd know that machine intelligence has exceeded human cognition when a computer could beat the best chess player in the world. You may remember when the IBM supercomputer Deep Blue beat Garry Kasparov, the World Chess Champion. That was in 1997.

The artificial super intelligence that exists today is superior to humans - but only in narrow ways. Chess computers are excellent at chess, but they don't do anything else. ChatGPT is great at generating text, but it just generates text. Midjourney produces fantastic images, but that's it.

Mikko Hyppönen

Principal Research Advisor F-Secure

"The phone you carry around in your pocket today would have been classified as a supercomputer just twenty years ago, in 2003. Supercomputers are the size of a small truck. They have their own power generator. And that phone in your pocket runs on a battery smaller than most wallets. In 20 years, the supercomputer has shrunk small enough to fit in your pocket. This is the future."

Artificial general intelligence - where self-aware computers surpass human brainpower - is the stated mission of OpenAI, the foundation behind the company that built ChatGPT. We are not there yet. We may be in a year, a decade, or even a century. And when it arrives, the benefits are going to be massive. It's going to cure cancer. It's going to cure all the diseases we have. It's going to fix the climate.

But even before we achieve superhuman intelligence and experience the enormous opportunities and risks of becoming the second most intelligent species on the planet, the AI revolution will bring us immense rewards - and inconceivable new challenges. We are more reliant on technology than ever, and AI affects computer security and privacy in unlimited ways.

AI enables the creation of completely plausible content of all kinds, including images, video, text, and audio. As a result, there will be deepfakes - images and videos digitally altered to put someone else's identity on another person's body - on dating sites. Romance scams will be supercharged by faked images. And large-language models, like the one that powers ChatGPT, will aid and automate phishing attacks and scams of all sorts.

> **“The AI revolution will bring us immense rewards - and inconceivable new challenges”**

Reality - as we knew it - is over. The revolution we're seeing right now may just be the beginning, but it has the power to reshape the world, for better or worse.

Very soon, it will be very difficult to discern what's real and what's not. This will become the overarching role of cybersecurity - assessing authenticity in a world of deepfakes. And it's a role we must take seriously. Because even if we see much of the future coming decades away, we can't control our creations, even if we wanted to.

The AI revolution that we're all watching happen right now is going to be a bigger deal than the internet, the single biggest technological revolution we have seen. Long after the last human has died, AI will still be around. And the future of this planet will depend on those of us who were alive when we first made superhuman intelligence.

> **"This will become the overarching role of cybersecurity – assessing authenticity in a world of deepfakes."**

## Meet the experts

We know how important it is to listen to the experts when it comes to cyber threats. So, this eBook is informed by expert insights from F-Secure's Principal Research Advisor Mikko Hyppönen, Threat Intelligence Lead Laura Kankaala, and Principal Consultant Tom Gaffney.

**Mikko Hyppönen**
Principal Research Advisor

**Laura Kankaala**
Threat Intelligence Lead

**Tom Gaffney**
Principal Consultant

# Intelligent machines hit the mainstream: A closer look at the emerging AI landscape

The first recorded use of the term "artificial intelligence" to describe computers that could emulate human thought came at an academic conference in 1956. But until recently, few humans had ever had an actual conversation with a robot. But that changed on the last day of November in 2022, when ChatGPT, a chatbot that instantly generates human-like text responses to just about any question, was released to the public. Within weeks, the app was spreading faster than just about any technology in recorded history. As of the summer of 2023, more than a billion people know exactly how it feels to talk to a machine.

## AI isn't an overnight sensation

"Generative AI - which produces text, images, music, and videos that often exceed the quality of those produced by humans - has existed long before the widespread popularity of ChatGPT," said Laura Kankaala, F-Secure Threat Intelligence Lead. "But there are certain tech-related reasons why we are seeing AI become increasingly more mainstream now."

AI requires heavy computing power and vast storage systems to handle the demanding operations, she noted. OpenAI, the foundation that produces ChatGPT, has been working on developing advanced AI and the infrastructure that supports it since 2015, a full seven years before the release of the chatbot that uses a large language model that was trained on a massive dataset that includes books, articles, and billions of web pages.

"The incredible popularity of ChatGPT along with the image generator Midjourney and a wide array of other AI-powered generators has made the possibilities of the technology much more tangible," Kankaala said.

## What is a large language model (LLM)?

Laura Kankaala explains: "As my colleague Khalid Alnajjar says, language models aim to generate text by understanding the context and predicting the most likely response to it, one word at a time. Think of the LLM as an experienced assistant, who has read through all the data and can provide you with relevant help for nearly any project or task."

# What is artificial general intelligence?

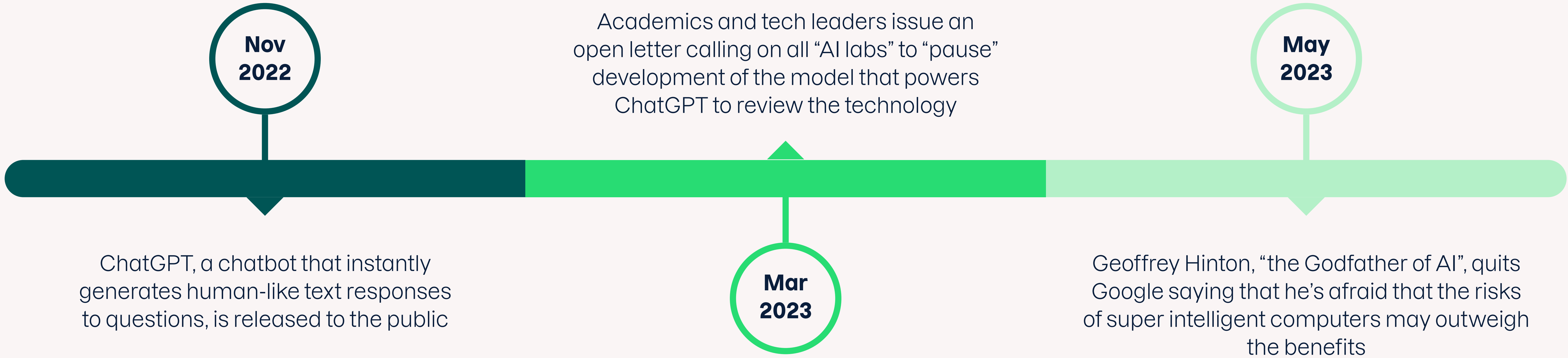
Artificial general intelligence (AGI) refers to when artificial intelligence can easily surpass human capabilities. Unlike current generative AI tools which offer 'narrow' forms of intelligence relevant to specific tasks, AGI will rival human cognitive function and intellect. We aren't there yet, but reaching AGI is the mission of OpenAI, creators of ChatGPT.

## The risks of AI are both theoretical and real

Not everyone is overjoyed about the startling progress of artificial intelligence. The fear of super-intelligent robots turning against their human creators is a theme that runs through various works of science fiction. Suddenly, these fantasies feel very real.

In March of 2023, a group of academics and tech leaders issued an open letter calling on all "AI labs" to "pause" development of the model that powers ChatGPT to review the technology before the development of what's known as "artificial general intelligence," where machine intelligence will easily surpass human capabilities. That warning was followed in May by computer scientist Geoffrey Hinton, colloquially known as "the Godfather of AI" quitting Google - which has been creating its own AI, including the chatbot Bard - saying that he's afraid that the risks of super intelligent computers may eventually outweigh the benefits.

Some experts believe a pause in the development of AI is unlikely, if not impossible, given the abundance of projects in development around the world. And predictions about the arrival of the artificial superintelligence that some experts fear range from years to decades.



Academics and tech leaders issue an open letter calling on all "AI labs" to "pause" development of the model that powers ChatGPT to review the technology

ChatGPT, a chatbot that instantly generates human-like text responses to questions, is released to the public

Geoffrey Hinton, "the Godfather of AI", quits Google saying that he's afraid that the risks of super intelligent computers may outweigh the benefits

Regardless of whether robots remain friendly to humanity after they surpass organic brain power, the economic and societal shifts that come from these machines rapidly gaining human intelligence will reshape society as we know it. And already, the dangers have begun to arrive. Officials from Singapore and Europol have issued warnings about the very concrete risks of generative AI in the hands of criminals and other bad actors.

### AI, like the internet, will be inescapable

"AI will transform our lives - it will affect all types of industries and initiatives, such as research into medicine, or even climate change," Kankaala said. "It can change our societies for the better, as long as we make sure we have safeguards in place. AI can be a personal assistant that is embedded in different everyday applications we use - such as tools that help us stay protected online."

It's almost harder to imagine products that won't have AI functionality in the future than those that will. A survey commissioned by IBM in 2022, before the launch of ChatGPT, found that nearly half of companies, 44%, were looking to implement AI in their businesses. That percentage has now surely spiked dramatically, as this technology is likely to become as ingrained in commerce as the internet itself.

Those of us alive right now will remember what life was like before we ever had a conversation with a robot - or had robots anticipate, meet, and even eliminate our needs. However, there will be fewer of us every day. Meanwhile, the intelligence of machines will only grow.

> **"It's almost harder to imagine products that won't have AI functionality in the future than those that will."**

## How does AI currently shape our lives?

To truly understand both the risks and opportunities that this technology presents, we need to understand that AI has already been shaping our lives for years.

- Recommendation engines that power social media sites, streaming services, and online retailers have long been powered by the precursors of what we now call AI
- GPS navigation tools have become better at picking optimal routes using AI
- Internet-connected home devices such as Amazon's Alexa and Echo have been made more useful by their ability to process information in a manner similar to humans

Laura Kankaala

Threat Intelligence Lead F-Secure

"Cyber criminals will exploit AI the way they have the world wide web, email, mobile devices, and social media – that is, in any way they can."

# Artificial intelligence, real threats: The impact of AI on cyber threats and how to stay ahead

AI will likely be the most important technological development of our lifetime, as Mikko Hyppönen noted. But as with any new digital technology, the development of AI and related technology will create and complicate existing cyber security and privacy concerns.

"Of course, as with any new groundbreaking technology or innovation, there is a huge risk of misuse, unethical behavior, and potential environmental and societal impact," Kankaala said.

The same technology that's likely to transform industries ranging from software to education to health care, will also give cyber criminals powerful new advantages when it comes to creating scams, malware, and threats we can't even imagine yet.

"At worst, powerful AIs can become tools not only for cyber crime, but for those who wish to affect power dynamics within a society and shatter modern democracies," she added. "Its capabilities for surveillance and monitoring should not be overlooked."

While the mainstream AIs developed by organizations like OpenAI and Google will always include guardrails that aim to prevent their misuse, criminals will always find a way to weaponize a powerful tool.

"Attackers that are good at social engineering, or the art of manipulation for malicious ends, will likely find ways to exploit any large language models."

# Phishing and Smishing

## How AI makes this more effective

WormGPT was identified in the summer of 2023 in a forum connected to cyber crime. This AI platform reportedly produces incredibly effective messages that aid criminals hoping to commit Business Email Compromise (BEC), one of the most profitable forms of online fraud in the world. While this malicious alternative to ChatGPT is focused on enterprises, it's also extremely effective for constructing phishing or smishing attacks that steal individuals' private data or trick victims into installing malware

Even without this customized tool, generative AI apps like ChatGPT can be used to improve the effectiveness of phishing and smishing attacks. Thanks to the natural language processing in large language models, a chatbot can write a professional-sounding email or text message in seconds. All criminals need are a few keywords to get started.

"What generative AI can already do is make all of these attacks more convincing," Kankaala noted. "This gives criminals a slight edge, and they'll take any edge they can get."

The bots can proofread the text of scam emails, automatically eliminating grammar and usage errors. She adds that thanks to AI, phishing attacks will only get more sophisticated, customized, and, eventually, automated.

"Soon, you should expect an automated multi-step process where the first communication will have no links to a phishing page, no request to do anything specific but just very authentic text that initiates a conversation," she said. "And before you know it, you're hooked."

EXPERT TIP

"If you aren't among the hundreds of millions that have tried ChatGPT, take the time to try it out. When you experience firsthand how convincing a conversation you can have today with an AI, it will probably help you be more careful when you engage in a chat with an unknown party over the internet. This awareness alone could help you avoid potential phishing attacks."

**Laura Kankaala,**
Threat Intelligence Lead

**Tips for staying secure**

Since generative AI is advancing so quickly, it's more important than ever to make sure to use strong passwords and multi-factor authentication to protect your accounts from potential scammers. It's also important to proactively protect devices from malware with endpoint protection, as scammers could try to get access to your data via a malicious program.

EXPERT TIP

"Beware of any unexpected or unusual demand for money. If someone is asking for gift cards, cryptocurrency, or a wire transfer out of the blue, you should be aware that these methods are used to make payments difficult or impossible to track. So, whenever you can, buy yourself the most important resource - time. Do whatever you can to take a break and do a little Googling about the situation you're in. You may find that it's not as unique as it first feels."

**Laura Kankaala,**
Threat Intelligence Lead

### Tips for staying secure

Fighting these sorts of tailored voice scams requires people to do something that goes against our best instincts. In the era of AI, we must be - at first - skeptical of everything, even contact from the people we love most. If you find yourself in a situation where a friend or family member needs money instantly, take a breath. Remember that now almost everything - from a person's voice to an image to a phone number - can be spoofed. If you can, call the person directly. You may confuse someone or interrupt a deep sleep. But at least you won't have let criminals take advantage of your best intentions.

# Vishing

## How AI makes this more effective

Imagine this. You get a voicemail in the middle of the night. It's the voice of a cousin, an aunt, even your child. And, the voice is begging you to send thousands of dollars immediately or your loved one may be trapped in jail with no bail money. It feels like a nightmare, so you act fast. But you soon find out - hopefully before you send any actual money - that the audio is faked, the product of AI.

Research suggests the number of vishing attacks has been on the rise for years, long before many of the popular generative AI tools were widely known and available. While there isn't evidence yet of widespread abuse of AI audio tools in scams, there will continue to be examples of targeted attacks utilizing faked voices.

"As the power of generative AI becomes more accessible and they require even less existing voice sample data for copying someone's voice, these very tailored voice attacks may become far more common," Kankaala said.

# Privacy concerns

## How AI exacerbates these

AI tools come with the same sort of privacy concerns that arise from any popular online service, along with some unique and somewhat baffling issues that even science fiction authors may not yet have considered.

A data leak from ChatGPT in May of 2023 forced the company behind the chatbot to take the tool down briefly. That breach of over 100,000 accounts is now being investigated by the Federal Trade Commission. Of course, any company that stores private data digitally - which is almost every company on earth - will likely have to deal with a data leakage eventually. But the unique relationship AI can have with users has already led to some increasingly complex concerns.

In May of 2023, Samsung banned the use of ChatGPT on company devices and networks after a few employees apparently fed confidential company data to the tool. The urge to disclose confidential matters to a generative AI tool makes a lot of sense given the intimacy such apps are designed to deliver. If a chatbot doesn't feel like a reliable, good listener, it won't gain or maintain much of a user base. And given that the point of large language models is to learn and extrapolate or approximate meaning based on the text it consumes, who can even imagine what these models might be learning from the words of the individuals who use them?

It's a lot to expect users to continuously make educated decisions about a groundbreaking technology that even some of its creators fear. This is why governments around the globe have begun to look at how AI could and should be regulated.

Italy briefly banned ChatGPT in the spring of 2023, prompting the tool to adapt to meet the country's regulatory requirements. And the founders and CEO of the foundation behind ChatGPT themselves called for regulation of "superintelligence" in a statement issued in May of 2023. However, a report from June of 2023 found that the same CEO had urged the European Union to adopt several amendments to the AI Act that would reduce oversight of the company's AI systems.

### EXPERT TIP

"We know that ChatGPT has become one of the most popular lures for cyber criminals seeking to spread scams and bad apps. And these same criminals would love to exploit the trust we're placing in AI-related apps given the chance. AI services are like any other service. You need to use strong, unique passwords to secure them. And the best time to start using a password manager is before your data is breached. So do that now if you haven't already."

**Laura Kankaala,**
Threat Intelligence Lead

### Tips for staying secure

The information you share with a generative AI tool occupies a strange place between webmail and social media. Ideally, the conversation you share with an AI chatbot will stay far more private than a post on X (formerly Twitter) or Facebook. But in reality, it may not. And we've all seen examples of email accounts being breached and published online. So, giving a chatbot secrets about your life or business could be as risky as documenting them in any online account.

While generative AI apps are designed for simple use, the privacy policies and settings are rarely as straightforward as the interfaces. It's worth taking the time to see both how the company expects to use your interactions and the tools they offer to limit how your information can be used in the future.

# Deepfakes

## How are these enabling cybercrime?

With AI, it's not only easy to mimic text and people's voices. With enough computing power and time, criminals can make fake images and videos that transpose one face onto someone else's body in almost any situation. These phony visuals are known as deepfakes.

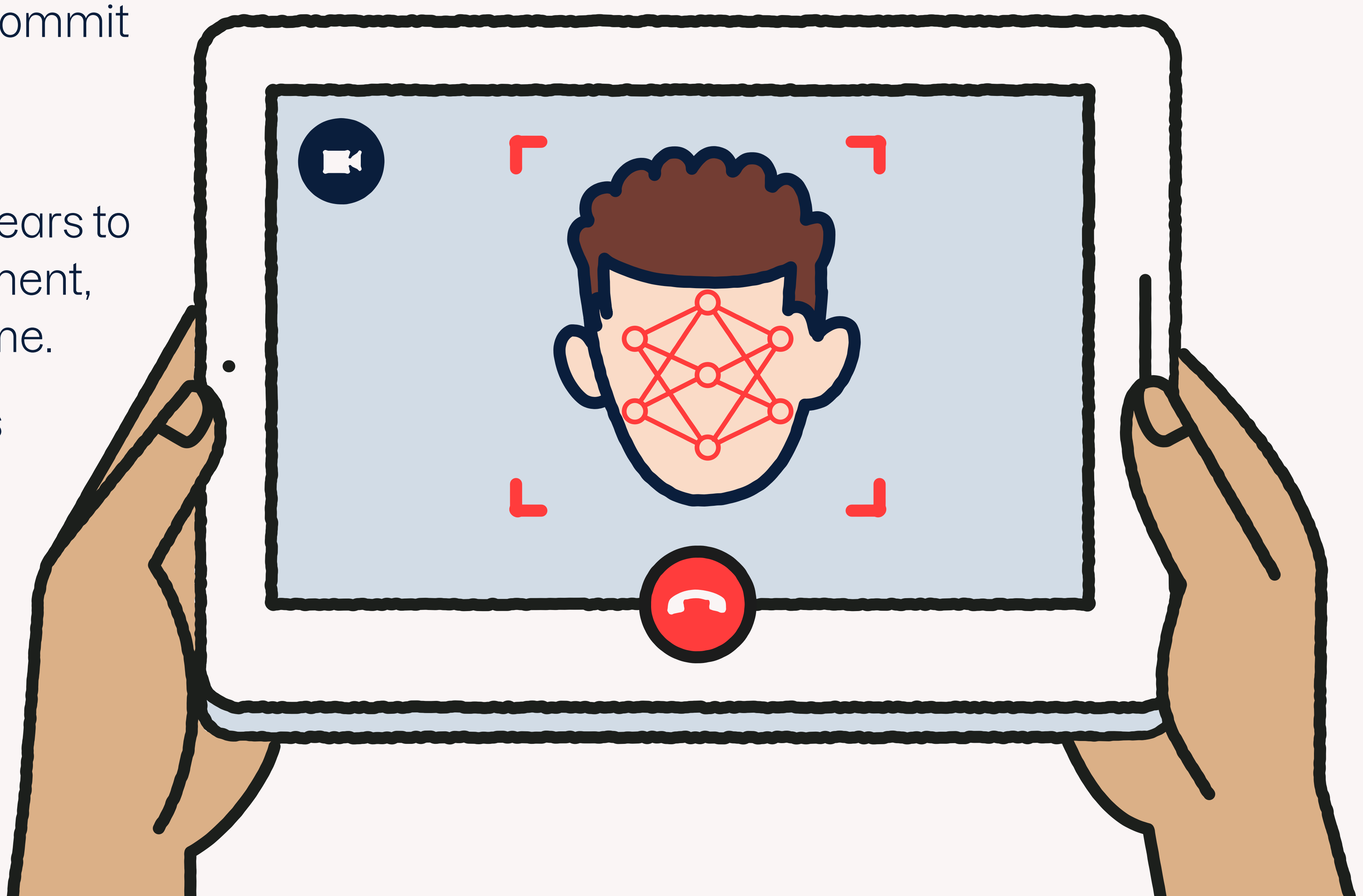
The Federal Bureau of Investigation (FBI) has issued warnings surrounding deepfakes since 2021. In June of 2023, it announced an uptick in malicious actors using this technology to create explicit content and commit sextortion. This includes the threat of exposing deepfaked videos to family and friends.

The growing availability of this technology appears to have led to an explosion of this form of harassment, which Kankaala notes has existed for a long time.

"This is often an overlooked issue, but it causes serious mental distress and sometimes even physical danger to non-consenting people, in particular women and worryingly minors, whose pictures have been used without their permission to create nudes, or their faces inserted in porn clips," she said.

And there is no real limitation to how these deepfakes can be used, whether for emotional abuse, political manipulation, or outright fraud.

F-Secure has already seen some examples of deepfake videos of Elon Musk on X (formerly Twitter) and TikTok talking about a cryptocurrency investment he's not involved with. Faked videos have also been used to directly ask victims for a payment to a charity or a get-rich-quick scheme. As the technology for this improves, not only will the number of these scam attempts increase, but the quality of them likely will too, making them increasingly difficult to spot.



EXPERT TIP

"The closest thing to an actual fix for deepfakes is simply not giving in to criminals' demands and reporting these incidents to law enforcement. The fact is that these criminals are going after multiple people at the same time, so they likely don't have the time to carry out their threats, such as digging up your family and friends to show them the faked images. And even if the criminals go that far, the only thing you can do is to warn your loved ones that they may see fake images of you naked. It's not ideal but it's far better than encouraging this kind of extortion."

**Laura Kankaala,**
Threat Intelligence Lead

**Tips for staying secure**

To avoid becoming a victim of deepfakes, the FBI suggests:

- monitoring the social media activity of your kids
- regularly searching yourself on the web
- locking down social media accounts' privacy settings and account security

Kankaala recognizes that posting images of yourself online is almost unavoidable today, but urges people to recognize that by doing this, there is a danger that they could be used in an illicit manner. While this doesn't prevent deepfakes, it does prepare individuals to take practical and calm steps to minimize damage should their images be abused.

# ID Theft

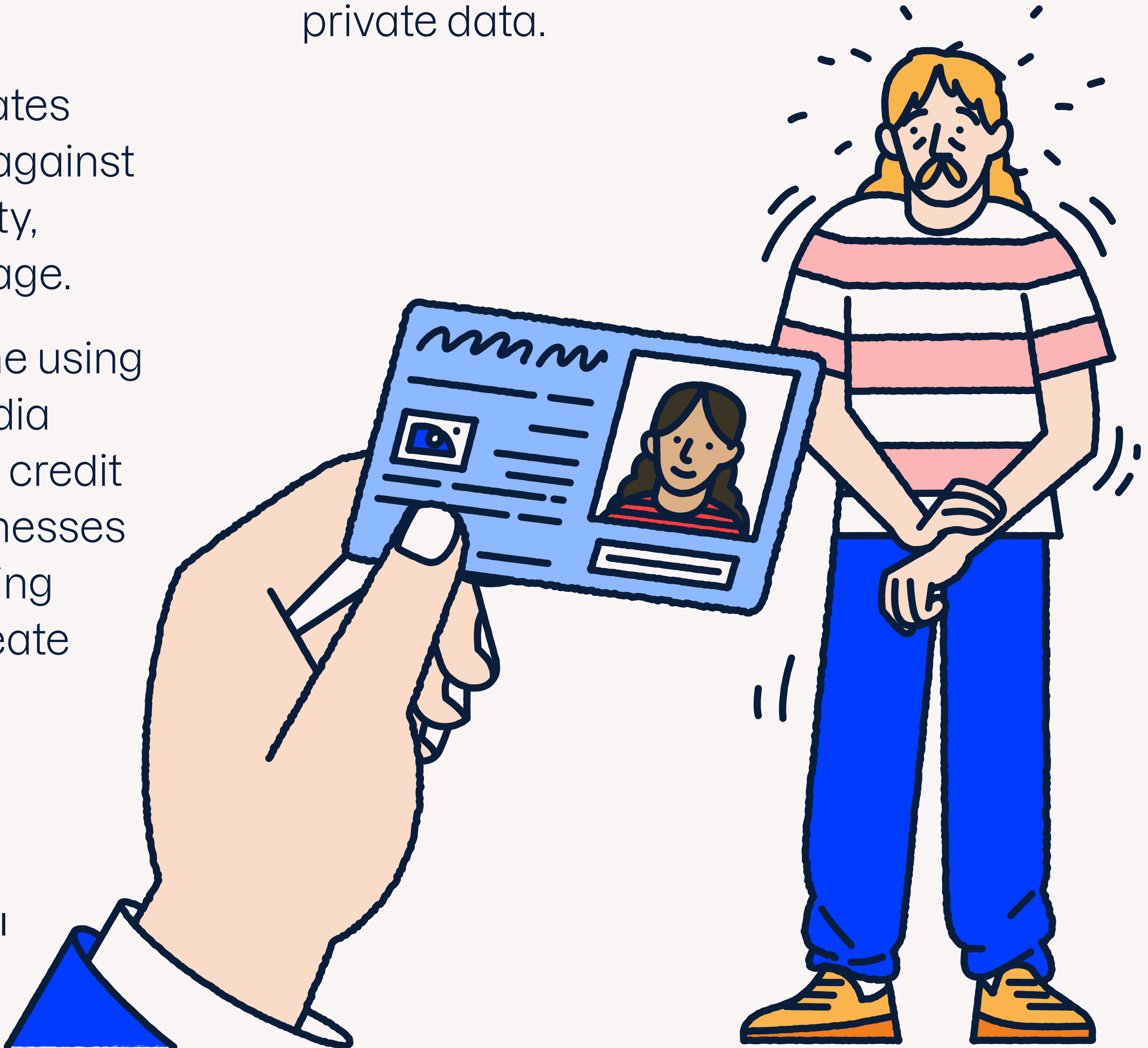
## How AI makes this more effective

Identity theft often refers to someone's actual private information being stolen and misused, for example to subscribe to services, buy things online, or even buy drugs with your credit card. But as the twenty-first century has unfolded, controlling one's identity has become much bigger than that.

The rise of generative AI complicates every individual's ability to guard against the exploitation of their individuality, whether that be their name or image.

ID theft could range from someone using your pictures for a fake social media profile, to someone misusing your credit card, or even setting up fake businesses in your name, possibly by combining real and fake ID information to create new and artificial identities.

Generative AI, like Photoshop and other powerful digital image software, has added to criminals' ability to create realistic images tied to real-world people. These can all be used to aid in the theft of an individual's identity without compromising any of their private data.



EXPERT TIP

"Much about the AI era feels like science fiction, but protecting yourself from identity theft in this time requires some old fashion homework. In addition to regularly using web searches, you must commit to always checking your financial statements. Whether you get them by mail or view them online, review all your purchases via credit cards every month, especially after you've done some traveling. In addition, check out your credit report at least once a year."

**Laura Kankaala,**
Threat Intelligence Lead

### Tips for staying secure

While the challenges of protecting your identity will only grow more complex in the age of AI, the tools that will protect your online and financial accounts are unlikely to change - at least for the foreseeable future.

The old advice about changing the password of any account from any service that may have been breached and never reusing that leaked password again still holds. In addition, placing a hold on your credit report, if such a hold is available where you live, remains essential if your key financial information - such as social security or account number - has been exposed. This prevents any new credit being issued in your name until the hold is removed by you.

Monitoring your data to see if it has been exposed in any data leaks remains essential. You can use a free tool like F-Secure Identity Theft Checker to check if your personally identifiable information has been shared on the Dark Web. And a solution like F-Secure Total includes identity protection that offers alerts and personal assistance if an online service you use has been hacked.

Just as AI has made the risks of identity theft greater, it also can and is being used by the good folk to improve internet security tools that prevent these sorts of crimes. So, make sure to use the best technology you can to protect yourself.

4

# Living with robots: The danger of AI-enabled devices and how to protect your smart home

While the rise in generative AI that we've seen over the past year is exponential, there's a good chance that you've been living with AI for years.

Smart assistants, such as Siri and Alexa, rely on natural language processing and machine learning - two cornerstones of AI. Both apps are voice-activated, which is another way to say that they're listening to you at all times, waiting to spring into action.

"It is clear and stated by their parent companies that Siri and Alexa both collect and may analyze the discussion between the voice assistant and its user." Kankaala said. "It's imperative to understand that any well-functioning AI needs good quality data for it to be trained."

## Filling our homes with robots

Roomba, the robot that vacuums your floors using smart maps it creates itself, has implemented artificial intelligence in a newer model. Mass market smart thermostats, mesh Wi-Fi routers, sound systems, home solutions, and lighting systems are all now using AI to offer users new features, comforts, and efficiencies. And AI has already been embedded in goods of all sorts – from hardhats on construction sites to agricultural robots to lug nuts on cars – to improve performance, safety, and durability.

Not every smart device in your home has AI and that will likely remain true for the near future. But any device that connects to the internet at least has some access to AI or related technologies. And many homes are overflowing with internet-connected devices.

According to Deloitte there are now 22 connected IoT (internet of things) devices in the average home within the United States. Analysts believe this number will continue to increase, with Statista claiming that by 2025 the number of connected devices in the average household will hit 34. This increase in connected devices poses a number of challenges that are heightened by the rise of AI.

Tom Gaffney

Principal Consultant F-Secure

# Why are smart homes so vulnerable? Cyber security expert Tom Gaffney explains

“In 2016, there were only a handful of IoT exploits,” said Tom Gaffney, Principal Consultant at F-Secure. “Today there are over 5,000.”

This is due, in part, to the newness of the technology. All software needs updates, especially software in its earliest versions. Unfortunately, many of the companies that got into making smart home devices didn’t prioritize security. Some devices couldn’t be updated at all. Other companies failed to issue fixes in a timely manner.

“The Mirai botnet in 2016 was a game-changing moment, because it focused the attention of cyber criminals on the connected home,” he said. “Mirai used a brute force password attack. It would use different password combinations - such as ‘admin’, ‘password’, ‘password 1234’, things like that - and there were so many IoT devices that failed in that security model, that it spread like wildfire, ultimately affecting 10s of millions of devices around the world.”

Some security experts have predicted the rise of AI-powered botnets that could learn and autonomously conduct attacks, mimicking human behavior. And given the security issues that exist in many internet-connected “smart” appliances, these devices will be an attractive target for these sorts of threats. Nation states, which have the most resources and intelligence to pour into cyber attacks, are certainly looking to compromise IoT vulnerabilities.

“Given how AI tools can encourage even greater intimacy and trust on smart home devices, they will only become more attractive to motivated attackers,” Gaffney added.

# Steps you can take to keep your smart home secure

- Make sure all your connected home devices, especially your Wi-Fi router, are protected with a strong, unique password
- Take the extra step of adding two-factor authentication to every smart home device where it is available
- Make sure only to welcome connected devices into your home that come from reliable manufacturers with a solid security reputation
- Retire any device - from webcams to Wi-Fi extenders - that doesn't continue to offer security updates
- Consider protecting every device in your home through your router or internet gateway by using a solution like F-Secure Sense offered by your internet provider

> **“For now, we need to be much more worried about bad people using good AI. And the only way to fight against that is with good internet security, awareness, and diligence.”**
>
> **Laura Kankaala,**
> Threat Intelligence Lead at F-Secure

# The future is not optional

It's important to remember that the potential good and usefulness of AI means it's likely to spread further and further into our lives, despite any risks it may present. So, avoiding generative AI tools in 2023 may be possible, just as it was possible to avoid using a search engine in the late 1990s. However, the ease and power of Google soon made search as essential as the internet itself. AI is likely to follow a similar path. As chatbots and image generators increase their utility, using them will become second nature - for both you and criminals.

“The cliché you will hear a lot is that only good AI can stop bad AI. And that's probably true, especially in the long run,” Kankaala said. “But for now, we need to be much more worried about bad people using good AI. And the only way to fight against that is with good internet security, awareness, and diligence.”

## Stay secure with F-Secure

As the age of AI evolves, protecting your digital moments and devices will be more important than ever. F-Secure Total makes this easy, helping you to secure your digital moments in a brilliantly simple way, today and tomorrow.

### With F-Secure Total, you can:

- Stay safe when banking, surfing, and shopping online
- Stop malware with top-rated antivirus software
- Protect your personal data online and prevent ID theft
- Safeguard your privacy with unlimited VPN
- Make the internet safer for your kids
- Protect your Windows PCs, Macs, and Android or iOS smartphones and tablets with one app

**Find out more about F-Secure Total today**

# About us

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 180 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit F-Secure today.

F-Secure®