# Cyber security for the AI age

As the digital world grows in power and complexity, so do the threats it faces. There is a constant arms race between cyber security and cyber criminals, both rushing to outcompete the other in sophistication. This means that the field of cyber security is rapidly growing and hungry for new talent that can understand the evolving threat landscape and respond accordingly by embracing new technologies, says **Dr Burcu Bulgurcu** at **Toronto Metropolitan University** in Canada.

**Dr Burcu Bulgurcu**

Assistant Professor, Department of Information Technology Management, Toronto Metropolitan University, Canada

Rogers Cybersecure Catalyst Research Fellow, Toronto Metropolitan University, Canada

**Fields of research**
Cyber Security, Information Privacy

**Research project**
Understanding human behaviour to promote cyber security and privacy practices

**Funder**
Canadian Social Sciences and Humanities Research Council

*This work is supported by the Social Sciences and Humanities Research Council (SSHRC) of Canada, under Insight Development Grant number 430-2021-01150. The contents are solely the responsibility of the authors and do not necessarily represent the official views of the SSHRC.*

PROFILE

Talk like a ...

## cyber security expert

**Cyber security** — the protections and measures taken against digital threats, namely cyber criminals

**Generative AI** — artificial intelligence that is capable of generating media (such as text or images). Generative AI uses models that learn from training data to generate new data with similar characteristics

**Malware** — software specifically designed to damage or criminally exploit a computer system

**Threat landscape** — the collective potential cyber security risks and dangers faced by a sector or individual

Today, more companies than ever are operating in the digital space. As organisations become increasingly dependent on online resources, they run the risk of being targeted by cyber criminals aiming to steal their assets, blackmail employees, or damage their business with malware, ransomware or other types of attacks. "Digitalisation is helping organisations to enhance communication and collaboration efforts, to innovate, and to stay competitive," says Dr Burcu Bulgurcu, a cyber security researcher at Toronto Metropolitan University. "However, without robust IT infrastructure and proper investments in security efforts, organisations lack the necessary backbone for security, leading to serious business vulnerabilities."

Burcu studies cyber security, but not in the way that involves delving deep into computer code. Instead, she studies how people's decisions affect their online security and privacy, and whether their behaviour can be nudged towards adopting stronger safeguards online. "I am interested in human-computer interaction and interface design," she says. "For instance, I designed app interfaces with different levels of privacy controls, to understand how availability of these controls affects user perception and concerns around privacy."

Cyber security breaches are rarely due to issues with the cyber security technology itself. Instead, they are caused by human error due to a lack of understanding and awareness of cyber security risks. Burcu's research findings are helping policymakers and educators incorporate the behaviours and motivations of technology users into their work.

### The threat landscape

Cyber security professionals refer to the cyber 'threat landscape', which describes the scope of identified and potential threats affecting a particular context, such as a sector or group of users. "The threat landscape evolves rapidly and constantly," says Burcu. Cyber security company BlackBerry reports that the healthcare and financial services are those most frequently targeted, as both hold large volumes of sensitive personal information that can be hijacked by criminals


to hold these services at ransom. Additionally, financial services also provide access to large sums of money, which criminals try to access through mobile banking malware.

There is evidence that cyber attacks have been increasing in recent years. "Every year, the numbers get worse and show that we are far from being able to mitigate and contain the numerous cyber threats that target both industry and government," says Burcu. "Organisations are increasingly under pressure to protect themselves, but many security professionals report that their organisations are not sufficiently prepared." Between March and May 2023, BlackBerry saw a 13% increase in cyber attacks involving new malware from the previous 90-day period. "This demonstrates that attackers are diversifying their toolkit to try and bypass defences," says Burcu.

An emerging and especially damaging form of attack involves targeting digital supply chains. Many organisations buy software from suppliers, which is then downloaded onto company computers. "Supply chain attacks happen when a cyber criminal compromises this software before the product reaches customers," says Burcu. "This provides an opportunity for the malware to reach several organisations at once, creating a ripple effect and potentially impacting thousands of victims." It is estimated that software supply chain attacks hit 60% of companies in 2021.

## The rise of AI

Artificial intelligence (AI) is a game-changer, and nowhere more so than within cyber security. "Both cyber attacks and our responses will become more intelligent due to generative AI," says Burcu. "In recent years, malicious actors have been employing AI to compromise corporate networks and interfere with business activities." AI can exploit a whole range of weaknesses – many human in origin – that previously were not available. "A generative tool, such as ChatGPT, can be used to generate a personalised phishing message based on a company's information and staff," says Burcu. "For instance, an AI bot can call an employee, using a deepfake voice that sounds like their boss, to ask them to transfer funds to a certain account."

> **"It's important to educate people on cyber security to raise awareness and establish responsible digital behaviour as a norm."**

Responding to these threats requires not only advanced technologies, but also training people to be aware of risks that previously did not exist. "It's important to educate people on cyber security to raise awareness and establish responsible digital behaviour as a norm," says Burcu. "Most people will easily trade a long-term goal, such as protecting their security, with a short-term goal, such as immediately accessing a digital resource." Most people readily accept the default privacy settings and security policies for apps or programmes without reading them. While people might say they are concerned about their privacy or security, their behaviour rarely reflects this priority.

## A holistic approach

"For the next generation of cyber security professionals, I believe that the most crucial skill to develop will be critical thinking," says Burcu. "This should be coupled with the ability to approach issues holistically, and to work collaboratively within an interdisciplinary team. Today's sophisticated attacks cannot be addressed with a one-dimensional approach." Burcu believes that it is vital for tomorrow's cyber security professionals to understand not only the technical side of the challenge, but also human behaviour and social sciences.

In Burcu's research, she uses both qualitative methods, which include interviewing people and analysing their responses, and quantitative methods, such as gathering data via surveys and social media and statistically analysing them. She conducts experiments to explore how people interact with different digital interfaces and what this means for their online privacy. She also analyses organisations' enterprise social media data by using advanced analysis techniques such as machine learning and natural language processing. This is to show that selected privacy settings of teams (and therefore whether organisational communications are private or transparent) can affect their performance, creativity and innovative output.

Achieving this breadth of knowledge is challenging, especially when the field is changing all the time, but Burcu says that is what makes cyber security and information systems so interesting. She enjoys understanding users' backgrounds and cultures, and unpicking the complex systems that govern our interactions with technology. "It's not just within cyber security that this holistic approach is needed," says Burcu. "Other professionals, such as doctors, will need to understand how to use digital technologies to support their patients and protect their sensitive personal information."

By ensuring that digital information and resources are kept secure and confidential, the next generation of cyber security professionals will be responsible for keeping us safe from cyber threats.

# Explore careers in *cyber security*

"Career options in cyber security are limitless!" says Burcu. Entry-level positions include IT or network support specialist, cyber security analyst or system administrator. With some experience, these roles can evolve into higher level positions, such as penetration tester, vulnerability analyst or cyber security supervisor. Other careers in the field include incident responder, security operations analyst, network security specialist, security architect, cyber security researcher or digital forensic analyst.

"There is a significant talent shortage in both technical and non-technical roles in the field of cyber security," says Burcu, which means cyber security professionals are in high demand. "In fact, they are in such demand that this might be one of the few scientific fields where a young person with a keen interest could secure employment without a traditional university degree." If you are passionate about cyber security, you could gain work experience and certification that could lead to a direct job in the field.

The skills needed for a career in cyber security are changing at an incredible pace. Creativity, critical thinking and communication skills are becoming more important than ever. "It's important that we, and future generations, leverage the latest advances, such as AI and other emerging technologies," says Burcu.

Cyber security encompasses many different fields, including non-technical roles. For example, for organisations to comply with the growing list of cyber security laws and regulations, they need lawyers and policymakers who understand the implications of cybersecurity and information privacy. "If you aspire to become a computer scientist or cyber security professional, it is still essential to understand the fundamentals of human behaviour and social sciences in our hyper-connected digital world," says Burcu. "In my work, for example, I investigate human behaviour and design user friendly interfaces that encourage people to adopt more protective behaviours."

## Pathway from school to *cyber security*

- At school, Burcu recommends studying computer science, information technologies (IT), mathematics, and programming. She also suggests finding courses that introduce you to networking, operation systems, risk management, information privacy, big data and ethics.
- At university, degrees in computer science and IT could lead to a career in cyber security. However, cyber security careers can also be obtained through non-technical programmes, such as business administration, management information systems or law. Most of these degrees have started to offer programmes related to cyber security, privacy, data protection, governance, criminology, digital forensics, legal research and compliance to prepare students for non-technical roles in cyber security.
- "You don't need to be highly technical to work in the field," says Burcu. "If you are interested in technology and willing to learn the fundamentals, you can find a way to integrate your background or interests into the field of cyber security."
- Currently, the talent gap is so big in the industry that you may secure a job in cyber security without a university degree. There are many official bodies with which you can gain qualifications and certification in cyber security, including ISC2 (**www.isc2.org**), CertNexus (**www.certnexus.com**), Global Information Assurance Certification (**www.giac.org**) and ISACA (**www.isaca.org**). "Toronto Metropolitan University offers a great security programme to qualify you to take the Certified Information Systems Security Professional (CISSP) exam (**www.isc2.org/certifications/cissp**) and other similar examinations, focusing on technical and managerial aspects of cyber security," says Burcu.

## Burcu's top tips *for staying safe online*

- Think before sharing something online. Rationally assess what you would gain or lose by releasing that information to strangers. Being conscious of your actions is the first step towards long-term safety.
- Take time to review and adjust the privacy settings on your social media accounts and electronic devices.
- Use strong passwords. Avoid using the same password on multiple platforms. Use a password manager to help you remember your passwords.
- Be aware of phishing attacks, including unsolicited emails, messages or links.
- Be cautious when downloading files from the internet.
- If you encounter any inappropriate or harmful content or behaviour online, report it to someone you trust, such as a parent, teacher or the police, and do not engage with it.


# Meet *Burcu*

**When I was younger, I enjoyed science and mathematics.** I was surprised when a high school teacher advised me to study something related to technology at university, because at the time (in 1998), the internet wasn't commonplace. I remember him saying, "Even kitchens will be equipped with computers in the future," and today, you can get a fridge that connects to your phone!

**At the age of 25, fresh from completing my education in Turkey, I took the bold step of applying for PhD programmes abroad.** I lacked academic connections to reach out to for guidance, but I was determined to make my dreams materialise. I was offered a PhD with full scholarship in Vancouver, Canada, and emigrated solo, leaving behind my family, friends and support system. Looking back, I reflect on the magnitude of that decision. For me, the courage I showed is my proudest accomplishment. This was a time when expressing myself in a foreign language and adapting to an unfamiliar culture were still uncharted territories, and leaving my homeland was a new experience.

**I decided to study cyber security and privacy at graduate school.** I realised how impactful rapid digitalisation could be, and how vulnerable it could make individual technology users, given technological advancements are always far ahead of policy, regulation and legislation.

**To my astonishment, my studies took me into the social sciences.** During my PhD studies in information systems, I found myself focusing on understanding human and organisational behaviours. It is fascinating to look into how technology affects our behaviour, and what underpins our motives. This involves not only conscious motivations but also the covert realm of unconscious beliefs and biases. This leads me to draw insights from disciplines such as business, psychology, neuroscience and organisational behaviour, as well as computer science.

> ***I lacked academic connections to reach out to for guidance, but I was determined to make my dreams materialise.***

**I quickly learnt the problem of cyber security is not just technical.** It also relies on social science, depending on awareness and training, so people understand the possible consequences of leaving digital footprints online by engaging with different technologies. By studying human behaviour, we can look into crafting user interfaces that help users make more informed choices. I'm fascinated by how we can design digital technologies to nudge users towards safer online actions, to protect them in the long term.

**These days, spending time with my two young children is my biggest enjoyment.** We like to be active and travel together as a family. I also enjoy yoga and painting for relaxation.

## **Burcu's** *top tips*

1. Embrace life's tests. You will inevitably encounter challenges and failures, but these can be rich with lessons that contribute to your growth and resilience.

2. Balance aspirations and flexibility. While it's important to set goals, it's equally vital to avoid them becoming rigid and unyielding. Being adaptable and flexible is indispensable for making the most of opportunities as they arise.

3. Embrace the rapidly changing technological landscape. Technology is reshaping our lives and opening new doors. AI is helping us tackle intricate challenges. Grasping this transformative power is essential for the next generation.