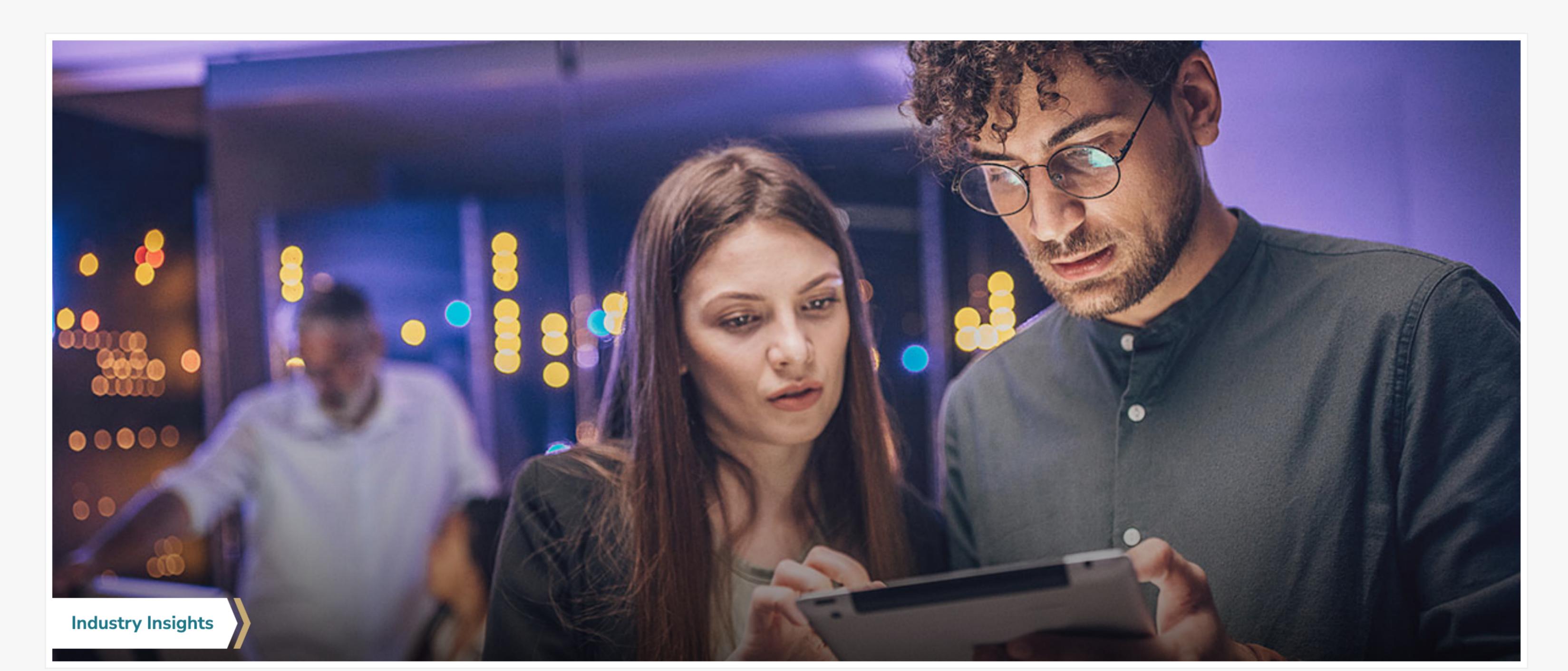# The Importance of Cybersecurity

Industry Insights

SHARE THIS ARTICLE

By Matt Rowley
Posted on October 8, 2024

An issue of rising national and international importance is the state of cybersecurity, and this is reflected in the growing job market for cybersecurity professionals. Everything in our personal, professional and civic life is connected to the internet – or likely will be soon – which brings incredible convenience along with great risk.

The aggregation of vast stores of personal data, the collection of sensitive information into remote data storage facilities, and uneven education about cybersecurity best practices have created a perfect storm of risk for individuals, organizations and governments. This has created a groundswell of interest, research and development in cybersecurity tools and in the people who create and use them.

In this article, we explore why cybersecurity is important in our modern-day society.

More Online Data Means More Potential Targets

The conveniences of cloud computing, automated support services, and other new technologies have accelerated efficiency for many processes, but they've resulted in a staggering amount of new data created and stored online. The amount of digital data created every day has grown by approximately 25% every year since 2012. Although a significant amount of user data is abstract, anonymized or proprietary, some of it includes things like credit card numbers, social security numbers, addresses, medical records and other sensitive information.

As this pool of data has grown, its value has not escaped the notice of criminals both domestically and abroad. Consider these highlights from Crowdstrike's 2024 Global Threat Report:

» Cloud environment intrusions increased 75% from 2022 to 2023.

» Cloud-conscious cases – meaning cases in which threat actors are aware of an ability to compromise cloud workloads and abuse features unique to the cloud – increased by 110%.

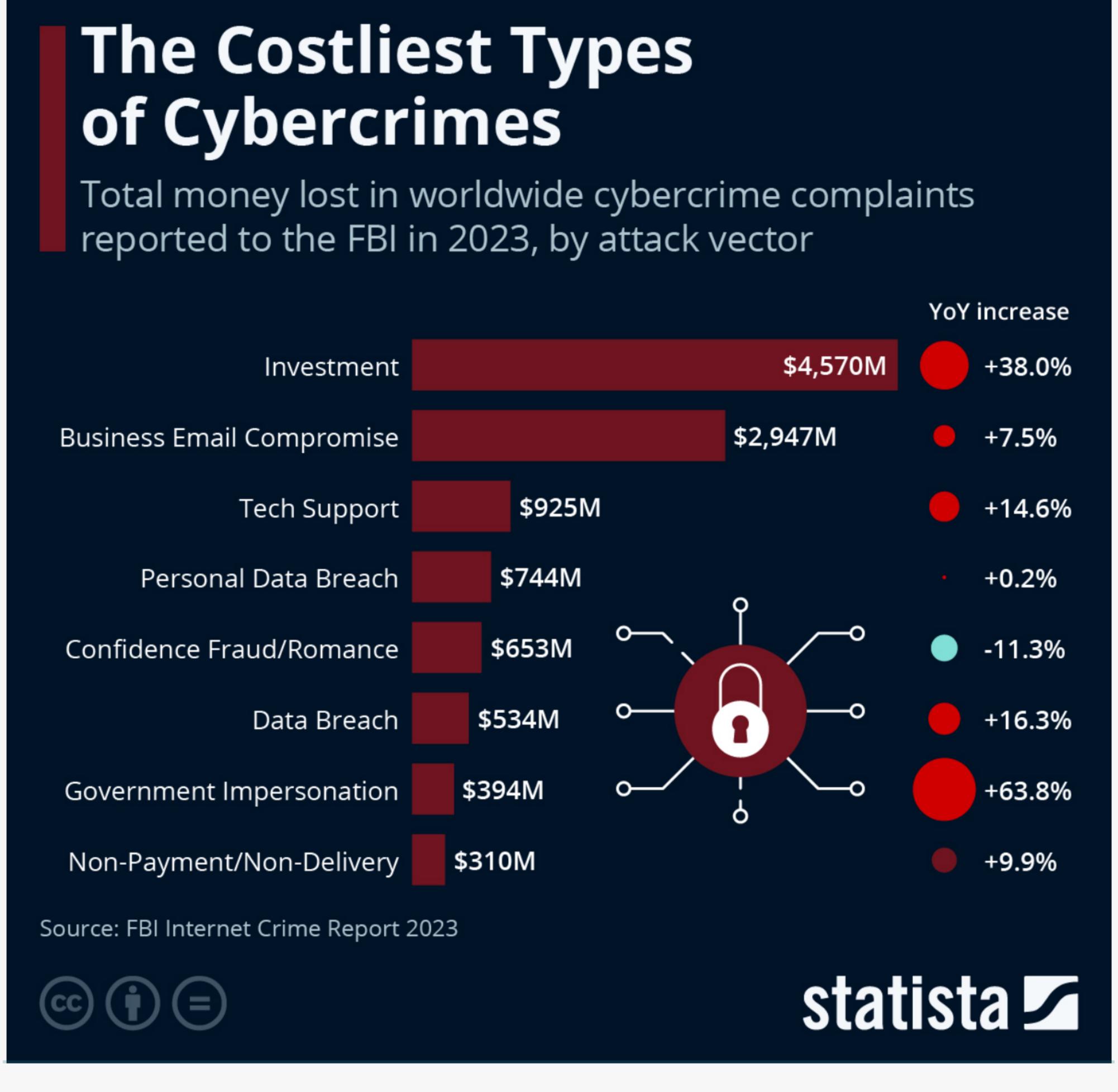## Personal Security Practices Create Risks

Organizations are making massive investments in cybersecurity, but in many cases their biggest risks come from their own employees. This doesn't necessarily mean that employees are intentionally being bad actors; stress and even altruism are some of the biggest reasons why employees may violate their cybersecurity policies.

Additionally, the younger generations – those who make up larger percentages of the workforce every year and often adopt new technologies enthusiastically – are often much less careful about their cybersecurity habits.

Related: How Human Behavior Affects Cybersecurity

$12.5 Billion in Financial Losses

The prospect of stealing hundreds or thousands of credit card numbers, social security numbers and other valuable assets has led to a massive – and costly – increase in cyberattacks worldwide. Statista reported that financial losses connected to worldwide cyberattacks totaled at least $12.5 billion in 2023, crossing the $10-billion mark for the second straight year. And as shown in the chart below, the two vectors with the largest totals lost were investment fraud and business email compromise.

The Costliest Types of Cybercrimes

Total money lost in worldwide cybercrime complaints reported to the FBI in 2023, by attack vector

Attack vector	Total money lost	YoY increase
Investment	$4,570M	+38.0%
Business Email Compromise	$2,947M	+7.5%
Tech Support	$925M	+14.6%
Personal Data Breach	$744M	+0.2%
Confidence Fraud/Romance	$653M	-11.3%
Data Breach	$534M	+16.3%
Government Impersonation	$394M	+63.8%
Non-Payment/Non-Delivery	$310M	+9.9%

Source: FBI Internet Crime Report 2023

statista

You will find more infographics at Statista.

Cybersecurity Education at CSU

So, what can cybersecurity professionals do to keep their knowledge up to date? In addition to monitoring industry trends and best practices, enrolling in a cybersecurity degree program is another good option.

Here at Columbia Southern University, our online degree programs in cybersecurity and information technology include the following:

» A.S. in cybersecurity.

» A.S. in information technology.

» B.S. in business administration, information technology concentration.

» B.S. in information systems and cyber security.

» B.S. in information systems and cyber security, homeland security concentration.

» B.S. in information technology.

» B.S. in information technology, data analytics concentration.

» M.S. in information technology.

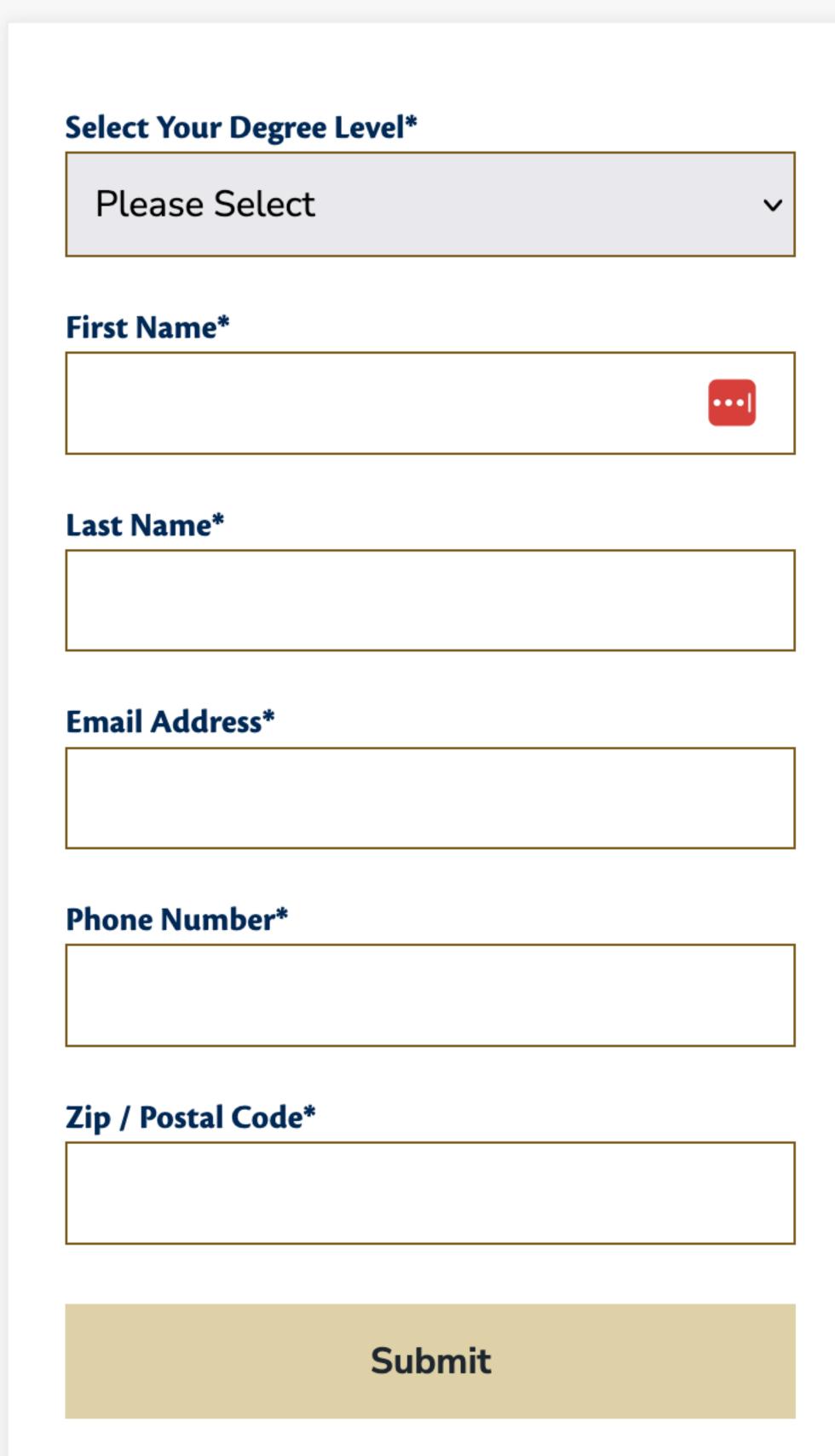To learn more about our online degree programs in cybersecurity, including some offering an Accelerated Path*, visit our website.

*Eligibility rules apply.

Multiple factors, including prior experience, geography and degree field, affect career outcomes. CSU does not guarantee a job, promotion, salary increase, eligibility for a position, or other career growth.

Request More Information

Select Your Degree Level*

Please Select

First Name*

Last Name*

Email Address*

Phone Number*

Zip / Postal Code*

Submit

By submitting this form you give Columbia Southern University consent to call, text and email you at the information above, including your wireless number if provided, regarding educational services. You may still choose to enroll in the university if you do not provide consent.