

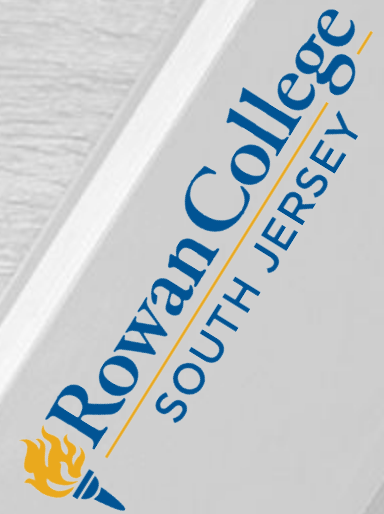
A blue oval graphic with white text is centered over a background image of hands typing on a laptop keyboard. The background also includes a pair of glasses, a small potted plant, and a book.

Professional Development Day Fall 2022

Josh R. Piddington

Vice President & Chief Information Officer

*Distance Education • Libraries • CTL • Web Dev • ERP • Innovation
Cyber Security • Network Ops • Project Management • Technology*

The logo for Rowan College South Jersey, featuring a stylized torch icon and the text "Rowan College" in a serif font and "SOUTH JERSEY" in a sans-serif font, all in blue and yellow colors.

Rowan College
SOUTH JERSEY



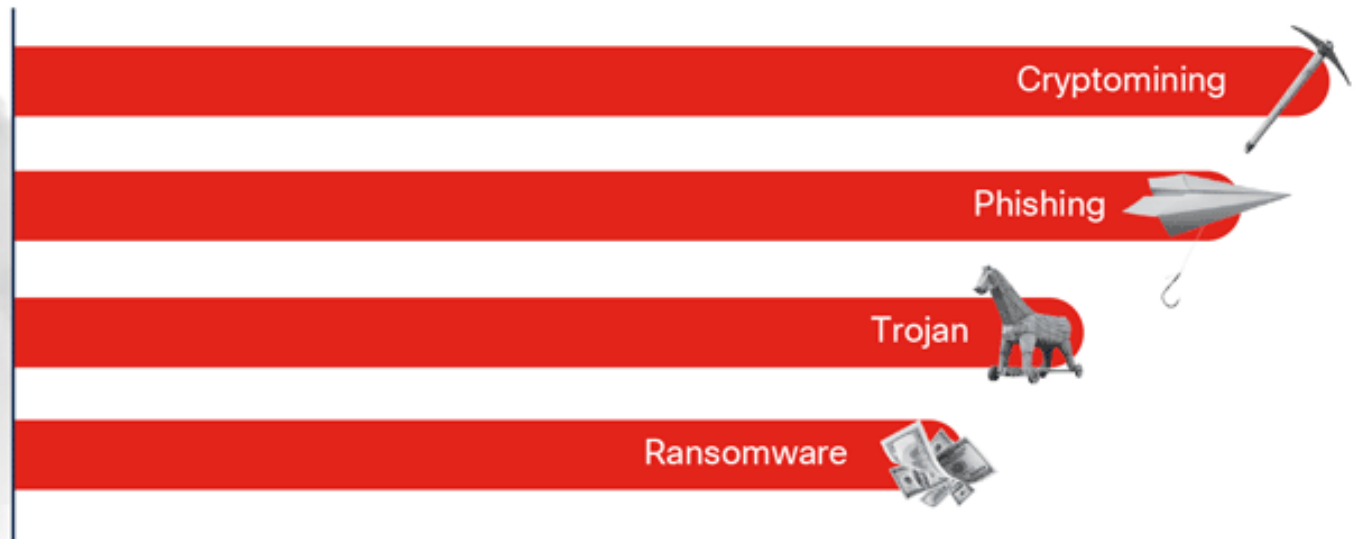
October is Cyber Security Awareness Month



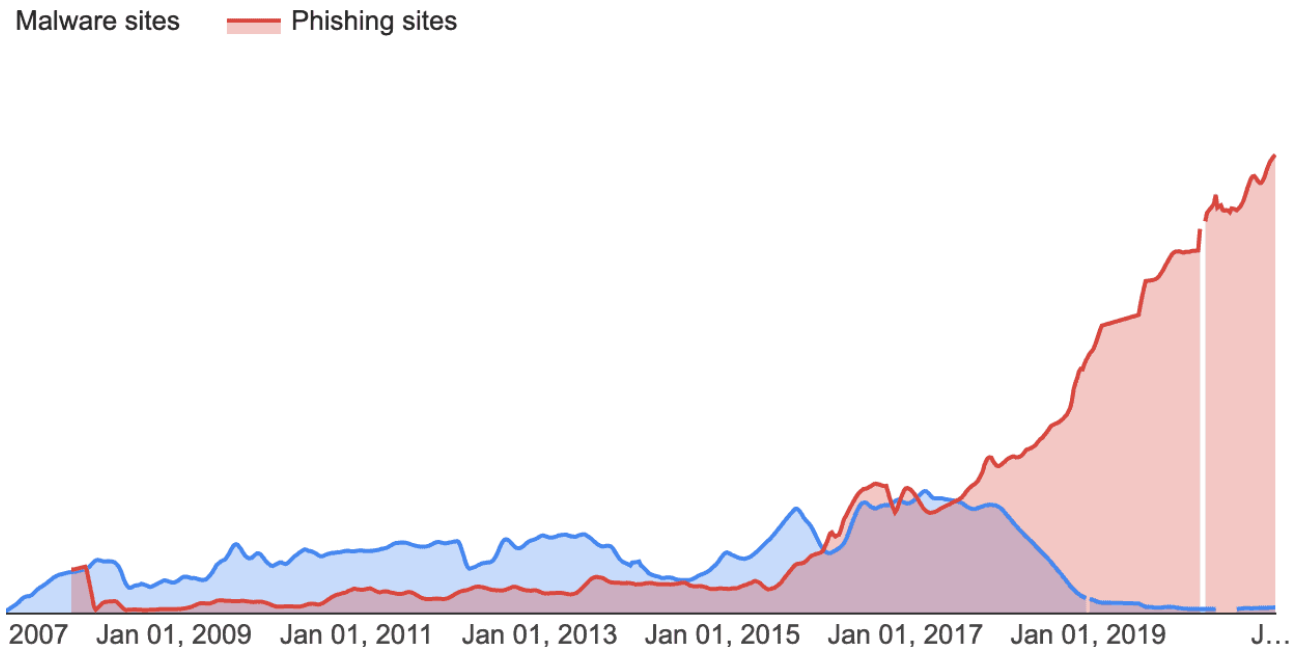
2022 Cybersecurity Threat Trends

10x

more queries than all other threat types



Prevalence of Phishing Websites



- [Google Safe Browsing](#) uncovers unsafe URLs across the web. The latest data shows a world-wide-web rife with phishing websites.
- Since 2016, phishing has replaced malware as the leading type of unsafe website. While there were once twice as many malware sites as phishing sites, there are now nearly **75 times as many phishing sites as there are malware sites**.
- Google has registered **2,145,013 phishing sites** as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (**up 27% over 12 months**).
- This compares to malware sites rising from 21,803 to 28,803 over the same period (**up 32%**).

The Most Targeted Industries

- Healthcare & Pharmaceuticals
- Manufacturing
- Education

75%



75% of organizations around the world experienced some kind of phishing attack in 2020.

\$3.92M

\$150 is the average cost per compromised record. \$3.92m is the average cost of a data breach.

96% of phishing attacks
arrive by email.

96%

An illustration of a hand holding a red smartphone. Above the phone is a white speech bubble containing the text '96%'. The background is a light gray gradient.

Phishing Awareness by Geography

- United Kingdom: 69%
- Australia: 66%
- Japan: 66%
- Germany: 64%
- France: 63%
- Spain: 63%
- United States: 52%

So what do we do?

- ⊗ Talk About It - October is Cyber Security Awareness Month
- ⊗ Required Phishing Awareness and Training
- Be Vigilant - Pay Attention to Email Details.
- Ask Questions - Did I Ask for this Attachment?
- ⊗ Utilize Technology like Microsoft Defender & Machine Learning
- ⊗ Multifactor Authentication
Student activating October 27, 2022
- ⊗ Self Phishing with Required Mediation

⊗ Required for Cyber Insurance Policies

Office 365 Safe Links



A link was clicked from a suspicious message.

This link was clicked from a message that has similarities to other suspicious messages.

We recommend that, before opening the website, go back and review the email message to determine the content of this email. Please be cautious when replying to the sender, even if it looks like someone you know.

[Tips for identifying phishing attacks](#)

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

[Learn more about Office 365 anti-phishing](#)



This website is classified as malicious.

Opening this website might not be safe.

`www.unsafe_url/login.php`

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

Powered by [Office 365 Advanced Threat Protection](#)

- Whenever an email is received from outside of the RCSJ organization, any links or URLs within the email will automatically be reviewed by Microsoft AI before being delivered to your inbox.
 - This review will help reduce the impact of any malicious or phishing emails that still arrive in your inbox.
- If the link or URL is determined to be suspicious or malicious after review, you will be redirected to a warning page that will appear like one of the following examples after clicking the link.

Office 365 Safe Attachments

- Microsoft will holistically analyze emails for malware that are sent through their services.
- Attachments that match known malware signatures will automatically be blocked from being delivered to your mailbox.
- From your perspective, these emails will never hit your mailbox.

Auto Purge

- If an email is determined to contain malware after it was delivered to your Inbox, the email will be retroactively pulled from all affected mailboxes.
- If received email is classified as **Phishing** or **Spam**, it is automatically sent to quarantine.
 - Daily Quarantine Emails are sent to your inbox for review