Are YOU CyberSAFE? Take our complimentary CyberSAFE Readiness Test.

Measure your organization's level of preparedness against cyber threats with the CyberSAFE Readiness Test. Comprised of 15 questions that are designed to measure an individual's knowledge of how to detect and avoid cyber threats, this complimentary assessment provides you with a tool to determine how well your organization is protected from imminent cyber threats.

SIMPLY FOLLOW THE INSTRUCTIONS BELOW TO TAKE THE CYBERSAFE READINESS TEST:

NEW CHOICE USERS

1. Go to http://cybersafecert.com and click Enter.
2. Under the New User section, enter **CRRD2BITLI** as your Access Key.
3. Click the Enroll button.
4. Fill in all required fields in the enrollment form, including your username and password. You will now be on the CyberSAFE CHOICE homepage.
5. Log in under the RETURNING USER with your newly created username and password.
6. Click the course tile for your course.

RETURNING USERS

1. Go to http://cybersafecert.com and click Enter.
2. Log in under RETURNING USER section with your username and password.
3. Click on the Add a Course tile.
4. Enter **CRRD2BITLI** as your Access Key.
5. Click the Enroll button.
6. Click the course tile for your course

HELPFUL HINTS

- Access Keys are case sensitive.
- Each Access Key can only be redeemed once.
- The password must be at least 6 characters with one being a number.
- Passwords are case sensitive in future logins.

Questions?
We're here to help.

NAME: Sana' Rasul
EMAIL: sana@hrgirlfriends.com
TITLE: Chief Instructor
TELEPHONE: (844) 474 - 4757

HRGIRLFRIENDS.COM/CYBERSAFE

cyberSAFE

[SECURING ASSETS FOR END-USERS]

> End-user awareness and training reduces security-related risks by 45% to 70%.
>
> — REUTERS.COM

CORPORATE BENEFIT

CyberSAFE allows organizations to increase their security posture quickly and with minimal investment by ensuring that end-users are equipped with the knowledge necessary to be good stewards of their organizations' data.

EMPLOYEE PROFILE

This course is designed for non-technical end-users of computers, mobile devices, networks, and the Internet, enabling employees of any organization to use technology more securely to minimize digital risks.

COURSE OUTCOMES

Students will identify many of the common risks involved in using conventional end-user technology, as well as ways to use it safely, to protect themselves and their organizations from those risks.

TRAINING CREDENTIAL

This course is designed to prepare students for the Certified CyberSAFE credential. Students can obtain their Certified CyberSAFE certificate by completing the Certified CyberSAFE credential process on the CyberSafeCert.com platform after completing this training.

HRGIRLFRIENDS.COM/CYBERSAFE

Get CyberSafe Certified

DURATION

3.5 hours (inclusive of the time required to complete the Certifed CyberSAFE credential process).

COURSE OUTLINE

LESSON 1:

Identifying the Need for Security

- Topic A: Identify Security Compliance Requirements
- Topic B: Recognize Social Engineering

LESSON 2:

Securing Devices

- Topic A: Maintain Physical Security of Devices
- Topic B: Use Passwords for Security
- Topic C: Protect Your Data
- Topic D: Identify and Mitigate Malware
- Topic E: Use Wireless Devices Securely

LESSON 3:

Using the Internet Securely

- Topic A: Browse the Web Safely
- Topic B: Use Email Securely
- Topic C: Use Social Networking Securely
- Topic D: Use Cloud Services Securely

EXAM / CREDENTIAL

CyberSAFE is accompanied by the Certifed CyberSAFE credential process. This brief online credential covers 20 questions, and is included as part of the courseware.

ENROLL

cybersafe@hrgirlfriends.com
hrgirlfriends.com/cybersafe

> “An investment in end-user awareness training reduces security related risks by 45 to 70%”
>
> — MARKETWIRED.COM

1. The average cost of a corporate data breach increased 15 percent in the last year to $3.5 million.
2. Each lost or stolen record containing sensitive and confidential information costs a consolidated average of $145.10.
3. Security incidents caused downtime of more than 8 hours for 31% of impacted organizations.
4. Companies in the U.S. paid the most at $246 per compromised record.
5. Mobile devices (smartphones and tablets) are perceived as the weakest link, closely followed by social media applications.
6. 49% of companies do not perform periodic fire drills to test IT Security event response plans.
7. Third parties with trusted access were responsible for 41% of the detected security incidents at financial services organizations.
8. 1 in 3 organizations do not know if third-party data access contracts / policies are in place.
9. Only 20% of IT security professionals are confident their organizations have made adequate investments in educating users on how to avoid phishing attacks.

PUBLISHED BY NETIQ.COM

HRGirlfriends

cyberSAFE
CYBER CREDENTIAL