SecurityRI.com™
We put the IT in Security

SecurityRI.com offers an extensive list of modules for all types of learners. The content of each module is regularly reviewed and revised to meet the training needs of our clients.

A preview of all current modules is available in the following list. Each module is available in a customized format for all levels of staff, industries and departments.

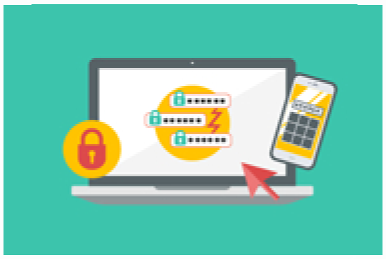
Malware Awareness

Learn to recognize the signs and symptoms of Malware exposure.

Malware is an abbreviated form of malicious software, is a type of software that has been particularly designed to gain access to or damage a computer, mostly without the knowledge of the owner. There are various types of malware, including computer worm, computer viruses, Trojan horse, adware, spyware, ransomware, scareware, and backdoor.

Malware mostly gains access to your device via the Internet and through email, even though it can also get access via hacked websites, music files, toolbars, game demos, free subscriptions, software, or anything else that gets download from the web onto a device which is not protected with anti-malware software.

Password Security



Although data breaches are out of your control, it's still imperative to create passwords that can withstand brute-force attacks and relentless frenemies. Avoiding both types of attacks is dependent on the complexity of your password.

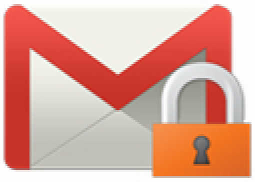
Password best practices are extremely important for securing accounts and data from those who wish to expose information. Learn the best ways to create new passwords that will remain secure into the future.

Social Engineering

Social engineering is the art of manipulating people, so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Recognizing these attempted manipulations is not difficult to learn and can go a long way to securing your data and network.

Email Security



Protecting access to your email account is just the beginning of securing your email. Being able to recognize malicious emails and the problems they can cause is just as important as having anti-virus software and a strong password.

Physical Security

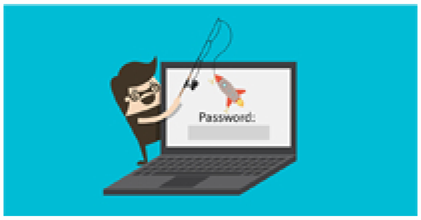
Is your place of business secure? Does your place of business have safeguards to keep an unwanted person or persons from physically accessing your computer network? Keeping your equipment safe and secure is just as important as having a firewall or Antivirus Software.

Mobile Device Security

Cybercriminals are continually looking for ways to exploit vulnerabilities in apps, operating systems, and software, trying to capitalize on security flaws before manufacturers find and patch them on mobile devices.

Since cybercriminals usually cast wide nets to reach more potential victims, mobile users should protect their devices early on to defend against threats. There are some easy steps that can be done to protect your mobile device at all times.

Phishing Awareness



Email is an essential part or our everyday communications. It is also one of the most common methods that criminals use to attempt to gain access to sensitive information.

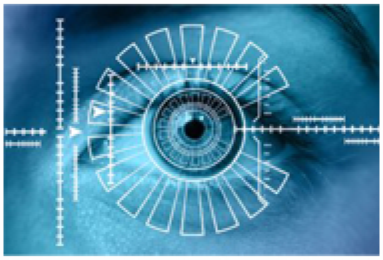
More than 90% of data breaches start with a phishing attack. Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading harmful attachments or divulging sensitive information, such as passwords, bank account numbers, and social security numbers. The ability to spot these emails is a vital skill for every employee.

Travel Security

Whether you're a regular business traveler, or a high-tech adventurer seeker, traveling—particularly abroad—poses unique cyber security threats. Business travelers are especially vulnerable because they often carry sensitive data, both personal and business related, on a variety of devices including smart-phones, laptops, and tablets.

With some simple and common-sense precautions, a traveler can reduce their vulnerability to a breach of sensitive data while traveling.

Information Privacy Awareness



Personal information is sometimes referred to as personally identifiable information (PII) or as personal data (the term used in the EU). Defining what personal information is — and being able to identify it — is essential for companies these days because privacy laws and regulations are triggered if personal information is involved. Personal information can be a tricky concept because it is sometimes contingent and contextual. what may not seem like a piece of PII can lead to other information that is sensitive. Keeping ahead of the criminals is very important.