

How to Submit Cyber Security Trainings

Purpose:

Provide employees the basic steps to use and complete submission of required cyber security trainings

Prerequisite:

- JRE account and password

Who's Responsible:

- All employees

Process:

- How to View Cyber Security Trainings
 - Navigate to Cyber Security Trainings app on Our Current, located on the Safety page
 - Click on View Cyber Security Trainings button



- Cyber Security trainings that need to be completed are listed under View Cyber Security Trainings
- The trainings that have been completed will indicate that the training has been "Submitted" in the Submitted column
- You can complete, review or amend a training by selecting the "View" button

All IT Cyber Security Trainings

| Topic | Month Of | Due By | Submitted | View |
|--------------------------------|----------------|-----------|-----------|----------------------|
| Sample Cyber Security Training | September 2026 | 10/1/2026 | False | View |
| Topic two | July 2026 | 8/1/2026 | False | View |
| Topic one | May 2026 | 6/1/2026 | False | View |
| Another Topic the third one | September 2026 | 9/25/2026 | True | View |

- How to Complete a Cyber Security Training
 - Navigate to the training you wish to complete, view or amend by clicking on the "View" button

All IT Cyber Security Trainings

| Topic | Month Of | Due By | Submitted | View |
|--------------------------------|----------------|-----------|-----------|----------------------|
| Sample Cyber Security Training | September 2026 | 10/1/2026 | False | View |
| Topic two | July 2026 | 8/1/2026 | False | View |
| Topic one | May 2026 | 6/1/2026 | False | View |
| Another Topic the third one | September 2026 | 9/25/2026 | True | View |



- At the top of the page, click the topic title link or the Attachment link to view the associated training



Click the Topic Title to View: [Sample Cyber Security Training](#)

Topic

Sample Cyber Security Training

Week Of

August 2026

Due By

8/1/2026

Attachment

[Monthly Training - Recognizing Phishing Emails.pdf](#)

Date Completed

Signature

Clear


Submit

- o Cover the information in the training document
- o Once done, close the training document

Sample Cyber Security Training x Microsoft Word - Monthly Train x +

PDF Viewer chrome-extension://oemmndcblbdoiebfnladdacbfmadadm/https... ☆

1 of 2 80%



PHISHING EMAILS

Definition – Phishing is when criminals send emails that pretend to be from trusted people or companies to trick you into clicking links, opening files, or giving away passwords or other sensitive information. Phishing emails might look like a message from IT, a bank, or a delivery company, but it is fake and meant to trick you into clicking a link or sharing information so attackers can steal from you.

What Attackers Do to Trick You and How to Spot It

Create urgency or fear – This makes you panic to act quickly then rush or skip verification.

- Examples: "Your account will be locked in 24 hours" or "Suspicious login detected" or "immediate action required"

Pretend to be someone you trust – it could be names/brands/companies/people that are familiar to you.

- Examples: A fake email from IT, HR, or upper management. A message claiming to be from Microsoft, PayPal, or Bank. Or an informal email from a trusted person such as, "Hi, this is the CEO-I need a quick favor."

Use look-alike email addresses or websites – One small character will be changed to fool your eyes as most people skim instead of reading carefully.

- Examples: PayPal (capital I instead of lower-case L), micr0soft.com, or company-support.com

Ask you to click a link or button they include in email - links or buttons that lead to fake websites, but the links/buttons feel safe and familiar.

- Examples: "Verify your account" or "View invoice" or "Sign Document."

Send unexpected attachments – files may be attached that contain malware or fake login pages as people are used to opening documents at work.

- Examples of PDFs: "Invoice.pdf" or "Secure_Document.html" or "Voicemail.zip"

Ask for sensitive information – information requests that no real company would ask for by email, but the request sounds routine and official.

- Examples: Passwords, MFA or verification codes, Social Security numbers, Credit card or bank details.

Use generic or slightly "off" language – vague and odd wording is used that doesn't seem suspicious right away.

- Examples: "Dear user" or "Hello customer" or any awkward grammar or unusual phrasing.

Pretend that something normal has changed – a routine process has been updated but no changes have been made.

- Examples: "Vendor banking details updated" or "New payroll system" or "Updated security policy"

Continues or reference existing conversations – reply to or mimic legitimate email threads that feel familiar and expected.

- Examples: "Following up on my previous email" or "As discussed earlier" – Even when no discussion happened

Try to avoid verification – excuses are given as to why they must avoid phone call or double-checks. This works because people want to be helpful and efficient.

- Examples: "I'm in a meeting" or "I'm traveling" or "Can't access my phone right now."

Phishing Email Example

This is a screenshot of a phishing email that was sent to many here at J. Ranck Electric. Please review the arrow locations and refer to corresponding explanations below the email example.

- o Sign your name in the signature box
- o Click "Submit" button



Click the Topic Title to View: [Sample Cyber Security Training](#)

Topic

Sample Cyber Security Training

Week Of

August 2026

Due By

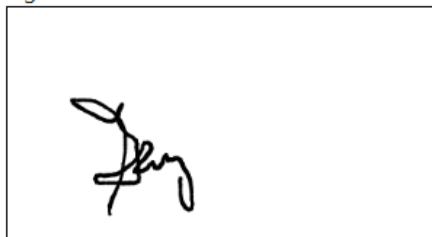
8/1/2026

Attachment

[Monthly Training - Recognizing Phishing Emails.pdf](#)

Date Completed

Signature



Clear

Submit

Troubleshooting:

- For technical issues submit a ticket to IT support@jranck.com
- For process questions send email to support@jranck.com

Revision #4

Created 22 April 2026 19:02:19 by gspiekerman@jranck.com

Updated 23 April 2026 18:27:20 by gspiekerman@jranck.com