



# DEPARTMENT NOTICE

22-070  
7/15/22

## Required Cybersecurity Training (Supersedes DN 21-015)

The City and County of San Francisco requires all employees to take cybersecurity awareness online training.

**To access the training, sign into the SF EMPLOYEE PORTAL, go to the “My Learning” tab and take the online Cybersecurity training.**

### What You Can Do to Reduce your Cybersecurity Risk

- Never share your user credentials for any application with anyone internally or externally.
- Utilize caution when you receive emails prompting you to enter user credentials, even if from a trusted source. When in doubt, contact the sender, ideally by phone or in person, to verify the email is valid. [REDACTED]


### Types of Cybersecurity Risk

There are two main categories of threats to our systems - Software Compromise and Social Engineering:

- Software Compromise – activist hacking groups, organized crime and nation state criminals are constantly probing software for security vulnerabilities, which allow the criminal enterprise to gain unauthorized access to computer systems. Software vendors continuously update their software to mitigate these vulnerabilities. [REDACTED]

- Social Engineering – this term, sometimes called impersonation attacks, is used for scams in which an individual impersonates a trusted person to manipulate unknowing staff into voluntarily providing access to resources, accounts, or funds. A victim will commonly receive a “phishing” email message. The Department of Technology deployed phishing protection into the Microsoft O365 email system, but some will slip through. Be very cautious of emails that seem suspicious.

Hackers are constantly adapting and so must we. Cybersecurity requires all of us to take an active role to prevent malicious groups from accessing our systems and data. [REDACTED]

  
WILLIAM SCOTT  
Chief of Police

*Per DN 20-150, all sworn & non-sworn members shall electronically acknowledge this Department document in PowerDMS. Members whose duties are relevant to this document shall be held responsible for compliance. Any questions regarding this policy should be made to [sfpd.writtendirectives@sfgov.org](mailto:sfpd.writtendirectives@sfgov.org) who will provide additional information about the directive.*