10-Minute Supervisor Trainings

Kentucky Soil and Water Conservation Commission

December 2014

SECURITY

Conservation districts are in possession of many types of sensitive information, and it is important that every type of information is protected from any one who might want to gain access to the district's data.

CYBER SECURITY:

Passwords

Access to district computers, email accounts, online banking accounts, etc. should be protected by secure passwords.

- Should contain at least 8 characters
- Should include a mixture of lower case, upper case, and special characters
- All passwords should be changed regularly
- At least one supervisor should have access to the district's passwords. This supervisor should be one who is bonded.
- Passwords should NOT be written on sticky notes and easily seen.

Phishing emails

It is important that anyone who receives and sends districts emails should keep a healthy dose of skepticism when opening and answering emails.

- These are emails through which hackers are trying to gain digital access to the district
- Your bank or the government will NEVER email you to ask for account details
- If you have any doubts about whether a company's email is legitimate, call that company to ask
- Do NOT use the telephone number from that email to call – look the correct number up online
- Never open attachments from someone you don't personally know or are expecting an attachment from
- If people get an email from you that you didn't send (those emails asking your friends to send money), change ALL of your passwords immediately
- Look for misspelled words, altered logos, and incorrect domain names (@ky.com isn't the same as @ky.gov)

OFFICE SECURITY:

Locked Filing Cabinets

Conservation districts end up with paper copies of the district's financial information, as well as personal information from the district's customers.

- Anything with private information should be kept locked up
- This includes forms with customer's social security numbers, banking information, addresses, etc.
- The district's financial information includes copies of Quickbooks/Quicken reports, checks, credit cards, etc.
- Certificates of Deposit (CDs) and similar documents should NOT be kept in the office. These should be kept in the district's safe deposit box.
- At least one supervisor should know where the key to the filing cabinet is kept.

Workers, IT people, etc.

People come into and out of the district asking for access to different parts of the building. It's important to keep your skepticism for these people, as well.

- Don't trust who they say they are – always ask for identification
- If you are not expecting the service person, call the office to make sure
- Anyone left alone in the office should have passed a background check
- If you have NRCS equipment in the office (computers, servers, etc.), do not give anyone not previously approved by NRCS access to that equipment
- Don't give anyone your passwords. IT professionals should not ask for them – they'll ask you to enter your password when they need it

General Office Security

- Arrange office space so unescorted visitors can be easily noticed
- Keep offices neat and orderly to identify strange objects or unauthorized people more easily
- Don't leave purses, wallets cell phones, tablets, or other valuables in plain view
- Be aware, be proactive. If you think something might be amiss, then report it