

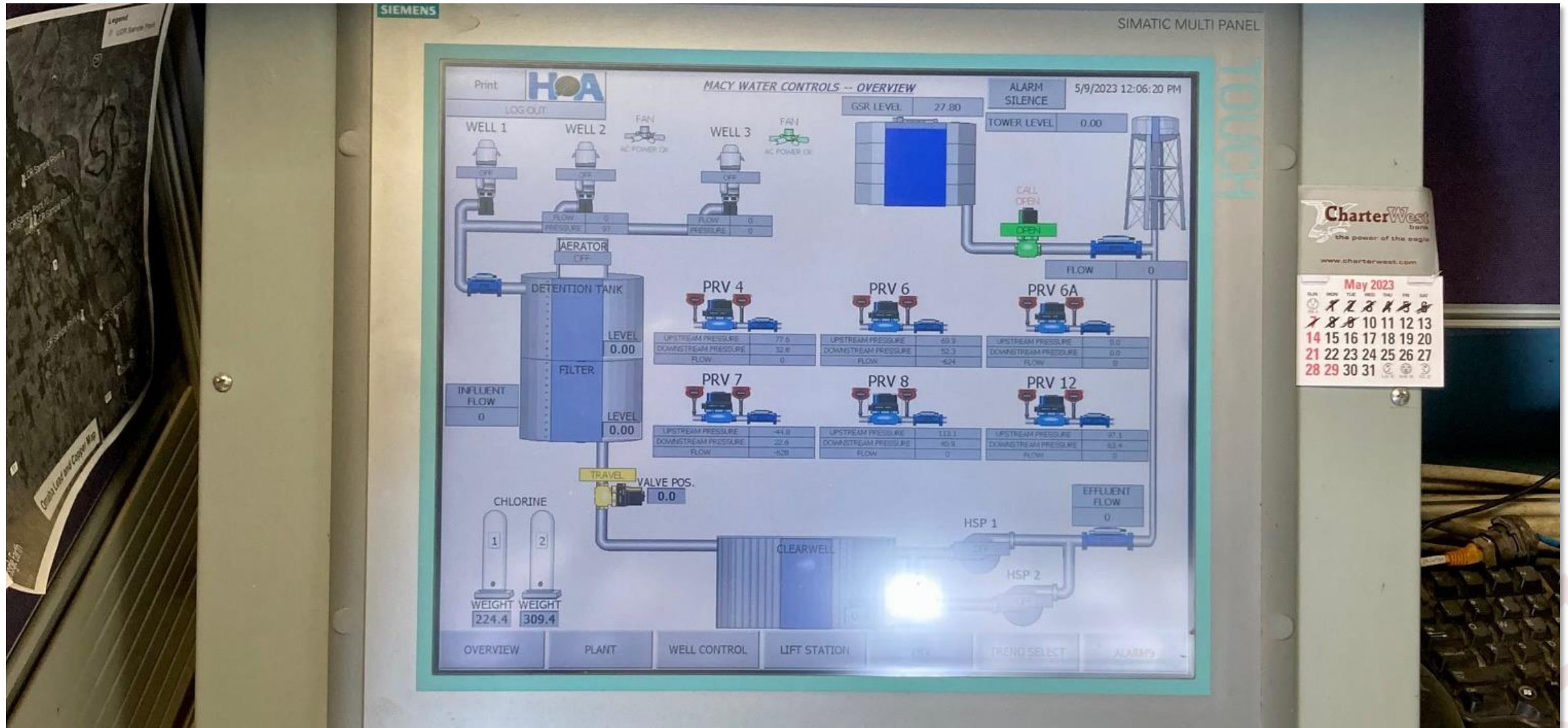
# Utility Cybersecurity

Glenn Barnes



WATER FINANCE  
ASSISTANCE

# SCADA Hooked Up to Internet?





# Computer Hooked Up to Internet?



# Smartphone?



To provide our  
service, we need to  
be prepared for  
**emergencies**





# Threats from People





# The New Threat from People—Cybersecurity



# What Can Hackers Do

- Mess with your treatment processes
- Steal utility data including financial data
- Steal customer data including financial data
- Lock you out of your files until you pay them



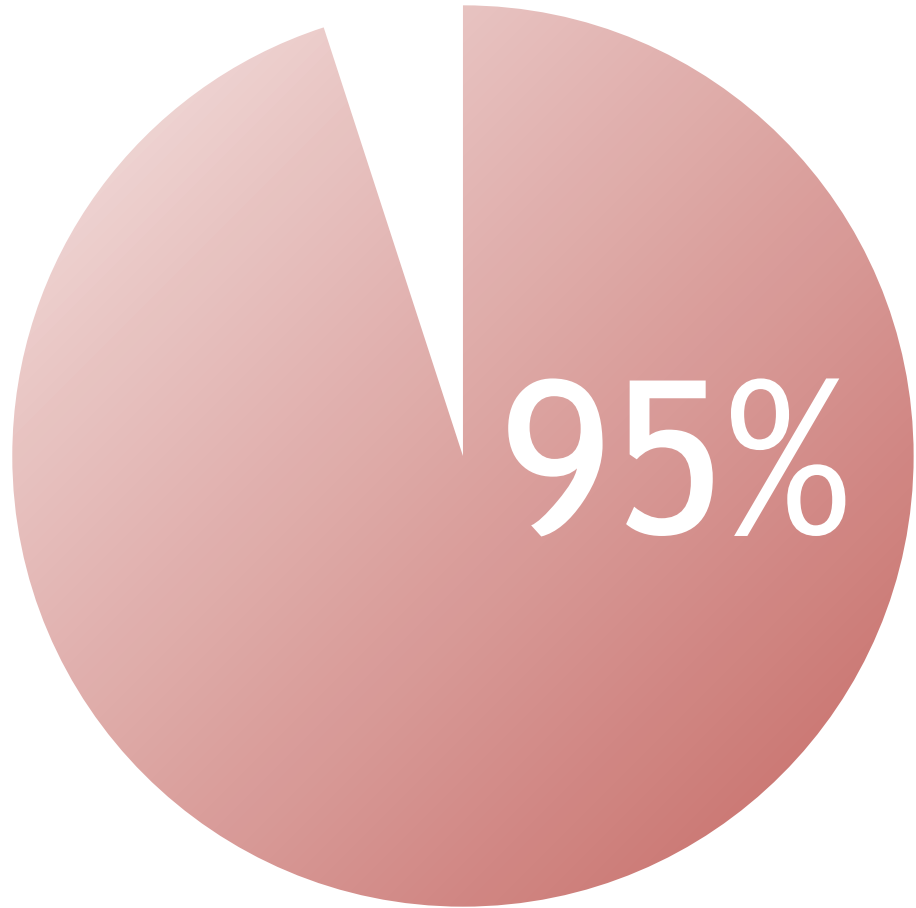


The **biggest cybersecurity threat** to my organization is...





It's me!



of cyber breaches  
are due to **human  
error**





# Passwords Exercise!

What do you think is one of the **10 most popular passwords** in the United States this year?

Write it on the paper in front of you



# Top 10 Passwords

- 12345
- 123456
- 12345678
- 123456789
- 1234567890
- 111111
- qwerty
- qwerty123
- q1w2e3
- password



# How Do Hackers Get Your Password?

- They guess it





# Time to Guess Your Password

≤6 characters Instantaneously

8 characters 30 minutes

11 characters 35 years

12 characters 3,000 years

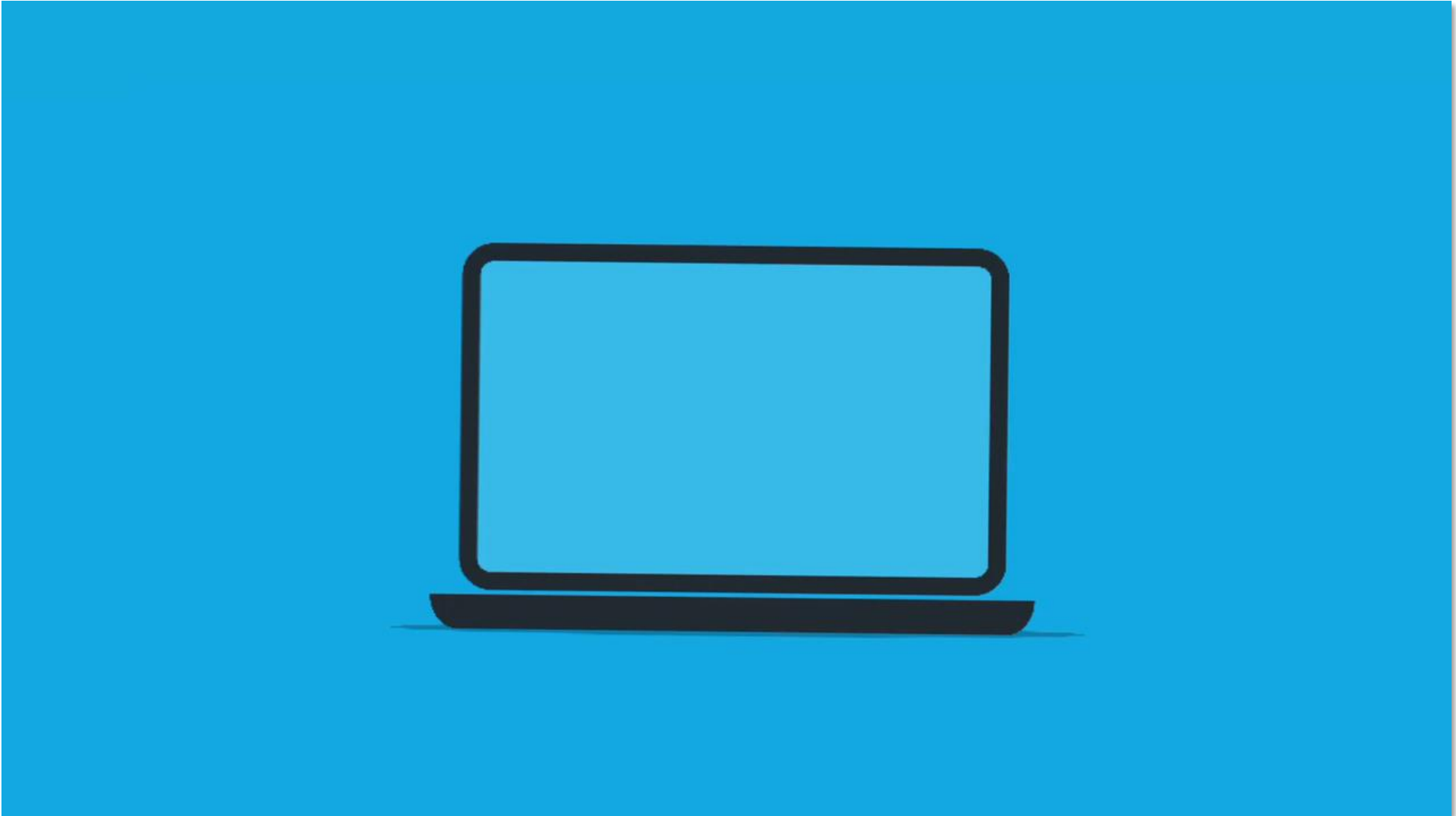
18 characters 438,000,000,000,000 years

# How Do Hackers Get Your Password?

- They guess it
- We give it to them



# Phishing





# Spot the Phishing Email Exercise!

- You have two printed emails in front of you. One is legitimate. One is not.
- With your neighbors, review each email and decide which is legit and which is phishing and **WHY** you think so
- Use everything at your disposal to check the emails, including your smartphone



## Email #2

To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent: Bager Meters Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and immediate action is required to prevent farther damage.

**Account Details:**

- Account ID: 1221809

## Email #2

To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent **Bager Meters** Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and immediate action is required to prevent farther damage.

### **Account Details:**

- Account ID: 1221809

## Email #2

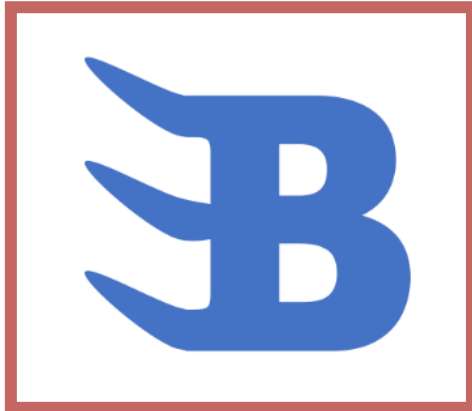
To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent: Bager Meters Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and immediate action is required to prevent farther damage.

**Account Details:**

- Account ID: 1221809

## Email #2

To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent: Bager Meters Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and immediate action is required to prevent farther damage.

### Account Details:

- Account ID: 1221809



## Email #2

To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent: Bager Meters Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and immediate action is required to prevent farther damage.

### Account Details:

- Account ID: 1221809

## Email #2

To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent: Bager Meters Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and **immediate action is required** to prevent farther damage.

### Account Details:

- Account ID: 1221809

## Email #2

To: Operator <[operator@grantvalley.gov](mailto:operator@grantvalley.gov)>

From: Account Manager <[bagers33235187@outlook.co.ng](mailto:bagers33235187@outlook.co.ng)>

Date: September 7, 2023

Subject: Urgent: Bager Meters Account Security Alert

---



Dear Customer,

We regret to inform you that your account security has been compromised. Unauthorized access has been detected on your Bager Meters account, and immediate action is required to prevent farther damage.

### Account Details:

- Account ID: 1221809

prevent farther damage.

**Account Details:**

- Account ID: 1221809
- Login Date & Time: 09/05/2023 06:11:26
- IP Address: 64.150.179.254

For your safety, we have temporarily suspended your account. To reactivate it and secure your personal information, please follow the instructions below:

**Action Required:**

1. Click on the following link to verify your identity and reset your account password:  
<http://satelliteintelligent.org/39565iW325904740GQ18796Bx51886Fp2773iL7691rr>
2. Enter your current login credentials and follow the on-screen instructions.

Failure to complete this process within the next 24 hours will result in permanent suspension of your account and loss of all data.

We take your security seriously, and we apologize for any inconvenience this may cause. Thank you for your prompt attention to this matter.

If you have any question or need assistance, please reply to this email immediately or call our support team at 296-718-4257.

Sincerely,

prevent farther damage.

**Account Details:**

- Account ID: 1221809
- Login Date & Time: 09/05/2023 06:11:26
- IP Address: 64.150.179.254

For your safety, we have temporarily suspended your account. To reactivate it and secure your personal information, please follow the instructions below:

**Action Required:**

1. Click on the following link to verify your identity and reset your account password:  
<http://satelliteintelligent.org/39565iW325904740GQ18796Bx51886Fp2773iL7691rr>
2. Enter your current login credentials and follow the on screen instructions.

Failure to complete this process within the next 24 hours will result in permanent suspension of your account and loss of all data.

We take your security seriously, and we apologize for any inconvenience this may cause. Thank you for your prompt attention to this matter.

If you have any question or need assistance, please reply to this email immediately or call our support team at 296-718-4257.

Sincerely,



prevent farther damage.

**Account Details:**

- Account ID: 1221809
- Login Date & Time: 09/05/2023 06:11:26
- IP Address: 64.150.179.254

For your safety, we have temporarily suspended your account. To reactivate it and secure your personal information, please follow the instructions below:

**Action Required:**

1. Click on the following link to verify your identity and reset your account password:  
<http://satelliteintelligent.org/39565iW325904740GQ18796Bx51886Fp2773iL7691rr>
2. Enter your current login credentials and follow the on-screen instructions.

Failure to complete this process within the next 24 hours will result in permanent suspension of your account and loss of all data.

We take your security seriously, and we apologize for any inconvenience this may cause. Thank you for your prompt attention to this matter.

If you have any question or need assistance, please reply to this email immediately or call our support team at 296-718-4257.

Sincerely,

prevent farther damage.

**Account Details:**

- Account ID: 1221809
- Login Date & Time: 09/05/2023 06:11:26
- IP Address: 64.150.179.254

For your safety, we have temporarily suspended your account. To reactivate it and secure your personal information, please follow the instructions below:

**Action Required:**

1. Click on the following link to verify your identity and reset your account password:  
<http://satelliteintelligent.org/39565iW325904740GQ18796Bx51886Fp2773iL7691rr>
2. Enter your current login credentials and follow the on-screen instructions.

Failure to complete this process within the next 24 hours will result in permanent suspension of your account and loss of all data.

We take your **security seriously**, and we apologize for any inconvenience this may cause. Thank you for your prompt attention to this matter.

If you have any question or need assistance, please reply to this email immediately or call our support team at 296-718-4257.

Sincerely,

prevent farther damage.

**Account Details:**

- Account ID: 1221809
- Login Date & Time: 09/05/2023 06:11:26
- IP Address: 64.150.179.254

For your safety, we have temporarily suspended your account. To reactivate it and secure your personal information, please follow the instructions below:

**Action Required:**

1. Click on the following link to verify your identity and reset your account password:  
<http://satelliteintelligent.org/39565iW325904740GQ18796Bx51886Fp2773iL7691rr>
2. Enter your current login credentials and follow the on-screen instructions.

Failure to complete this process within the next 24 hours will result in permanent suspension of your account and loss of all data.

We take your security seriously, and we apologize for any inconvenience this may cause. Thank you for your prompt attention to this matter.

If you have any question or need assistance, please reply to this email immediately or call our support team at 296-718-4257.

Sincerely,

A few **easy steps** can **greatly limit** your  
cybersecurity risk



# Passwords

- Change default passwords
- Make sure that your passwords are secure—long and complex
- Everyone has their own password
- Consider using a password management service that generates passwords that are virtually impossible to crack





Requiring **strong, unique passwords** is the single **most important step** for cybersecurity



# Access

- Limit system access to only those who absolutely need it for their jobs
- Limit system access from mobile devices especially to only those who absolutely need it for their jobs



# Access

- Disable access for former employees or former contractors/vendors/consultants **IMMEDIATELY**
- This was the issue in the Ellsworth County, KS incident



U.S. Attorneys » District of Kansas » News

**Department of Justice**

U.S. Attorney's Office

District of Kansas

SHARE 

FOR IMMEDIATE RELEASE

Thursday, October 21, 2021

## Kansas Man Pleads Guilty to Water Facility Tampering

TOPEKA, KAN. – A Kansas man pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County. Wyatt Travnichek, 23, of Lorraine pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access.

According to court documents, the Post Rock Rural Water District hired Travnichek in January 2018, and his duties included monitoring the plant after hours using a remote login system. Travnichek resigned his position in January 2019. On March 27, 2019, the remote log in system was used to shut down the plant and turn off one of its filters. Investigators established Travnichek's cell phone was used to perpetrate the intrusion, and that the phone was in his possession at the time of the shutdown. He told investigators he was intoxicated and didn't remember anything about the night of March 27, 2019.

# Require Multi-Factor Authentication

- When you log in, you have to enter your password and also confirm your identity a different way, such as entering a 6-digit number texted to your phone
- That way, even if someone gets your password, it is useless
- Most systems have this feature built in—you just have to turn it on





# Limit Computer Use to Work Purposes

- Limit staff ability to check personal email or to access websites not related to work
- **DO NOT CHECK YOUR EMAIL ON THE SCADA COMPUTER!**



# Ransomware: The Other Phishing Outcome



# How to Respond to a Cyberattack



# Disconnect Devices from the Internet

- Remove the connection between any device that may be impacted and the outside world
- Do NOT shut down computers or systems that may be infected—you may never get them back on again



# Document Everything

- Make note of the issues you are seeing
- Any suspicious emails
- Timelines, etc.



# Notifications

- Notify whoever handles IT for your utility, if you have anyone
- Notify utility and Tribal leadership
- Notify your information security vendor, if you have one





# Law Enforcement

- **Cyberattacks are crimes**
- Notify Tribal law enforcement
- Notify the FBI



<https://www.ic3.gov/>



FEDERAL BUREAU OF INVESTIGATION  
**Internet Crime Complaint Center IC3**

A large, light blue icon of an unlocked padlock is positioned on the left side of the central panel. The background of the panel is a dark blue gradient with faint, scattered alphanumeric characters in a lighter blue color.

## Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant.

[File a Complaint](#)



# Resources on Cybersecurity for Water & Wastewater Utilities







## Cybersecurity

[Cybersecurity Training & Exercises](#)

[Cybersecurity Summit 2020](#)

[Cyber QSMO Marketplace](#)

[Combating Cyber Crime](#)

[Securing Federal Networks](#)

[Protecting Critical Infrastructure](#)

[Cyber Incident Response](#)

## CYBER HYGIENE SERVICES

### Reducing the Risk of a Successful Cyber Attack

Adversaries use known vulnerabilities and phishing attacks to compromise the security of organizations. The Cybersecurity and Infrastructure Security Agency (CISA) offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

- **Vulnerability Scanning:** Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Web Application Scanning:** Evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- **Phishing Campaign Assessment:** Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
- **Remote Penetration Test:** Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable

<https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector>

## EPA Cybersecurity Best Practices for the Water Sector

Like other critical infrastructure, the water sector can be a target of cybersecurity threats and hazards. Implementing cybersecurity best practices is critical for water and wastewater utilities. The resources below can bring your utility one step closer to cyber resilience.

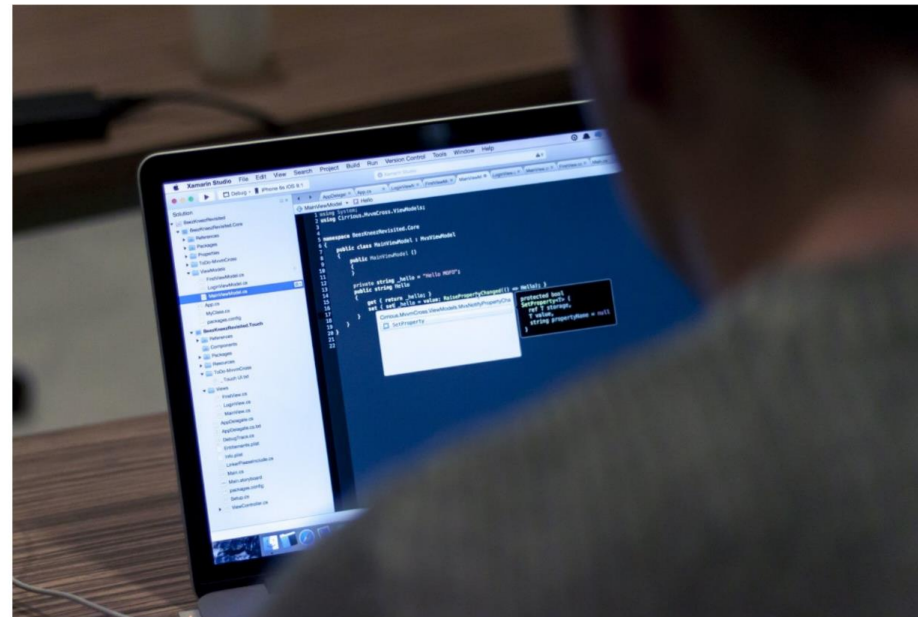
### Cyber Resilience Resources

**[Water Sector Cybersecurity Brief for States](#)**: This guide can assist state technical assistance (TA) providers with assessing cybersecurity practices at water and wastewater systems and developing an improvement plan to reduce cyber risks.

**[Cybersecurity Incident Action Checklist](#)**: This guide provides steps for water and wastewater systems to prepare for, respond to, and recover from a cybersecurity incident.

**Water Sector Cybersecurity Technical Assistance Provider Program**: This program trains state and regional water sector TA providers to assess

cybersecurity practices at water and wastewater systems and guide systems through developing a cybersecurity action plan to reduce risks and enhance resilience. The program includes follow-up assistance opportunities after the original assessment. For more





# Incident Action Checklist

- EPA guide on how to prepare for, respond to, and recover from a cyberattack

- [https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity\\_form\\_508c.pdf](https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf)



## Incident Action Checklist – Cybersecurity

*For on-the-go convenience, the actions in this checklist are divided up into three “rip & run” sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the “My Contacts” section with critical information that your utility may need during an incident.*

### Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers’ personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility’s website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes



Cyber incidents can compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence and result in financial and legal liabilities. The following sections outline actions drinking water and wastewater utilities can take to prepare for, respond to and recover from cyber incidents.





<https://www.waterisac.org/resources>

## WaterISAC RESOURCE CENTER

AWIA Risk Assessments  
and ERPs

COVID-19  
Resources

Cybersecurity  
Fundamentals

Perch Cyber Threat  
Detection


Power Outage  
Resilience

WaterISAC  
Publications


Search


Filter by +

Reset

 Search tips

10247 total results

Sort by: **Date** Relevance  Tiles  List

 MEMBERS ONLY



Security & Resilience Update -  
Phishing Attacks Targeting Water &  
Wastewater Sector, Spring4Shell  
Updates, and More

APR 05, 2022 IN INTELLIGENCE



Security Updates Addressing  
"Spring4Shell" and Spring Cloud  
Function Vulnerabilities

APR 05, 2022 IN CYBERSECURITY



Threat Awareness – Borat RAT  
Malware

APR 05, 2022 IN CYBERSECURITY



Free technical assistance from ITCA for Emergency Response Plans and Risk Resiliency Assessments



# Thank You!



Glenn Barnes

Director

Water Finance Assistance

[glenn@waterfinanceassistance.com](mailto:glenn@waterfinanceassistance.com)

617-388-4404

