your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

# Cyber Security Cleaning

## By Freisi M. Alfonseca, Cyber Intelligence, MS-ISAC

Spring is in the air and the time has come again for some digital spring cleaning. Prior to ushering in the warmer weather, roll up your sleeves, and take time to perform a few digital chores. On this year's to-do list be sure to include: device and software inventory, software updates, secure device disposal, email inbox clear outs, and password updates.

It is becoming easier and easier to accumulate Internet connected devices. Just think about the number of laptops, phones, and smart devices in your office and home. If you're struggling to remember all of what you have, it's probably time to take a few notes from the building blocks of cybersecurity, the CIS Controls. Controls 1&2 lead you on the path to "know thyself" through the inventory of devices and the software running on them. Once those steps are complete and you know the lay of your lands, Control 4 advocates keeping your devices secure.

How do yo make sure all that hard work was not for naught? Updates are a necessary evil! Sometimes they take a long time, but it's all worth it in the end to ensure the security of your devices. Simplify your life by setting up automatic updates that run while you don't plan on using you device—this has the added benefit of ensuring you don't forget to update.

After inventorying the devices, you may find you have accumulated a miniature museum of obsolete technology! Yes, I am talking about the stack of eight-inch floppy disk and 56KB modem on your basement. If you decide that you would like to get rid of a few hunks of metal and plastic gathering dust, be sure to securely recycle them. All hard drives and components that contain sensitive data should be shredded or destroyed to eliminate the risk of a cyber threat actor getting their hand on the information. Perhaps you don't want to get rid of devices; instead, give them a facelift. Dispose of the unused apps and old downloaded items on them. Be sure to empty the recycling bin/trash bin to fully remove those files.

The security of your devices shouldn't be the only security concern on your mind. Social media accounts can be awesome, but you should be confident the information exposed to the public is appropriate and intentional. Be sure to review the security and privacy settings on your social media profiles to ensure they are suitable to your needs. Let us not forget about old emails, as our inboxes deserve a good scrub, too. During your spring cleaning, take the opportunity to clear out the emails sitting in your inbox, subfolders, and the trash folder. Then, make sure to also delete any emails containing sensitive information that is no longer needed or at the least, download that information to a safer location.

The spring cleaning process could not be complete without the updating of passwords! We're all guilty of it, holding onto a password for years at a time because it is so effortless to remember. Alas, this is a huge security risk, particularly if this password has been used time and ime again across accounts. If you haven't already head, NIST published a new digital authentication standards. This is especially important for accounts that bar access to financial information, personally identifiable information (PPI), and electronic health records. Make yourself a tall glass of lemonade and get cracking at making your new passwords!

These spring cleaning digital chores will help refresh your cybersecurity posture and will ease your mind, so you can enjoy the warm weather and fresh flowers.

# CYBER SECURITY ONBOARD SHIPS

**Cyber security is everybody's responsibility.**
**The information provided here gives advice on how your actions can help to avoid cyber incidents.**

## POTENTIAL THREATS

### KEEP UNAUTHORISED SOFTWARE AWAY FROM SHIP SYSTEMS!

- Scan for viruses and malware before you connect authorised USB memory sticks to onboard OT and other networked systems.
- Personal laptops, tablets, USB memory sticks or phones must not be connected to onboard operational systems.

## INCIDENTS

### BE PREPARED!

- Keep your crew and any passengers safe – train for what to do if important OT systems do not work.
- Know where to get IT and OT assistance.
- Report suspicious or unusual problems experienced on IT and OT systems.

## PASSWORD PROTECTION


### BE IN CONTROL!

- Use new passwords every time you sign on to a ship.
- Choose complex passwords with num6er5s, $ymbo!s, and some CaPiTaL letters. Be careful, you have to be able to remember them.
- Keep your user names and passwords to yourself.
- Change default user passwords and delete user accounts of colleagues who have left the ship.

## SUSPICIOUS ACTIVITY

### BE VIGILANT WHEN YOU COMMUNICATE!

- Only open emails or open attachments from senders that you know and trust.
- Know what to do with suspicious emails.
- Think before you share information on social media or personal email about your company, job, ship or the crew.

INTERNATIONAL CHAMBER OF SHIPPING · BIMCO · MPA SINGAPORE

**OT:** Operational Technology is the systems which are used to operate the ship.

**IT:** Information Technology is the systems used for office work, email and web-browsing.

# Scam of the Week: Fiendishly Clever Gmail Phishing You Need to Know


**Twitter user @_thp shared a recent phishing scam that they received; and it's so fiendishly clever that it's gone viral. They wrote: "This is the most clever phishing scam I've ever encountered and for a second it almost got me." Now, that is perhaps a bit exaggerated, but you have to admit it's something a lot of users will likely fall for.**

**Here is how this scam works. The victim receives a text asking whether they've requested a password reset for their Gmail account - and, if not, to reply with the word 'STOP'.**

**Employees who have not received any new-school security awareness training could likely fall for this social engineering tactic, and will respond with 'STOP'. Next, they are urged to send the 6 digit numerical code in order to prevent the password being changed.**

**Of course what is really happening is that the scammer has requested a password change on their account. That request sends a code to the real account owner to verify that they actually want the password changed. And by sending the attacker that code back, you're enabling the bad guys to complete the password change, and now they have access to the account and all the email.**

**I suggest you send this email to your employees, friends and family. You're welcome to copy/paste/edit:**

**"There is a new scam where hackers send you a text that asks you about a password reset on your gmail account, and if you did not, text STOP. This is a scam. The bad guys asked for that password reset and now want you to send them the authorization code! Don't fall for it.**

**Remember that Gmail or any other web email service will never ask if you *don't* want to do something with your account. You didn't ask for a password reset, so you shouldn't be asked about one.**

**Do not reply to the text (doing so will tell the scammers that they have reached a valid number). And to prevent losing your account to bad guys, it's a very good idea to have 2-step verification set up on your Google account."**