

CAI Northern Ohio Chapter

Quarterly Newsletter

IN THIS ISSUE

CAI Releases Revised Reserve Study Standards

The Latest on Installing EV Charging Stations in Your Condo/HOA

"Nightmare" Neighbor's Conviction Gives Condo Owners Relief

Cybersecurity Training Security and Culture



MESSAGE FROM THE PRESIDENT

On August 25th we have an informative CAI event which will include an opportunity for you to meet with our diverse Business Partners via speed dating. This concept will allow you to meet briefly with every Business Partner. It is my pleasure to participate as a representative of the Community Association Managers International Certification Board (CAMICB) which is the global authority responsible for the Certified Manager of Community Associations (CMCA) credential. The mission of CAMICB is to support homeowners in community associations by recognizing and promoting professional managers who have demonstrated a comprehensive understanding of their role.

CAMICB is the international certification body with oversight responsibility for developing and delivering the CMCA examination and the maintenance and promotion of the credential. CAMICB supports the community association management profession internationally by working consistently to effectively position the value of the CMCA credential with stakeholders. The CMCA examination is developed by a broad and diverse team of volunteer Subject Matter Experts (SMEs).

CAMICB is not an educational entity but is committed to offering resources and guidance to CMCA candidates that will position them for success on the examination. CAMICB supports managers from the start of their professional careers through retirement.

I hope to see you at the August 25th event and look forward to our "speed date" discussing why you should become a CMCA.

M. Katherine Bushey, Esq., President
Northern Ohio Chapter Community
Associations Institute

CAI Releases Revised Reserve Study Standards

June 5, 2023 – In response to the Surfside tragedy, the Community Associations Institute (CAI) compiled working groups to discuss public policy solutions aimed at keeping communities and their buildings safe. Following the development of public policy initiatives, CAI assembled a variety of industry experts to revise its Reserve Study Standards, accounting for the critical nature of building safety. Revised by a comprehensive task force of fourteen industry experts, including reserve specialists, association managers, board members involved in legislative committees, an attorney, and an accountant, these new revisions encompass three main areas.

1. Disclosing long-lived assets in reserve study reports – Though long-lived assets such as foundations and electrical systems may not need funding or maintenance within the 30-year scope of the reserve study (RS), they should be disclosed to your RS provider and included in the report to avoid future surprises that could lead to deferred maintenance. Your provider should provide useful life and cost information for these items even if they are not currently being funded for.
2. Regular preventative maintenance – During RS kickoff meetings, RS providers should ask and associations should disclose if they are or are not regularly maintaining components in their community, long-lived or otherwise. If a component is not being regularly maintained, it is unlikely that it will obtain its full useful life. Your provider will determine the appropriate estimated remaining useful life and create a funding plan that prepares for its replacement, which is especially important when the useful life has been shortened as a result of deferred or reactive maintenance.
3. Inclusion of inspections as a reserve expense – Primarily applicable to mid-rise and high-rise buildings, periodic structural engineering inspections should be included in the RS as a reserve expenditure when applicable. This is to ensure funding is available to maintain current and long-term building integrity and safety. Inclusion of any additional testing and inspections (pipe inspections, electric thermoscans, pond bathymetric surveys, etc.) should also be considered.

The task force, compiled in March 2022 and including Reserve Advisors' Northeast Regional Director, Michelle Baldry (PE, RS, PRA), met regularly to review and revise CAI's reserve study standards. Addressing condo safety and building integrity, the group adjusted the standards to enhance and encourage best practices to keep buildings sound and communities safe.

The Latest on Installing EV Charging Stations in Your Condo/HOA

Reprinted from *Community Association Management Insider*, July 2023

Times have changed since we last covered electric vehicle charging stations. A reader has new questions: “Do you have any research or papers on installing EV charging stations on condominium property? We’re trying to determine how much it would cost, whether grants are available, and whether we can charge a fee or make a profit on these EV station.”

Our experts share their most recent work with clients on EVs here.

Mostly Individuals, Some Communities

Our experts say their clients more often deal with individual owners who want to install an EV charging station rather than the association installing the station for the community.

“Florida has laws that require a board to approve an owner’s request to install an EV charging station if an individual owner wants to install it in a limited common element parking space or garage,” explains Jennifer Biletnikoff, a shareholder in the Naples, Florida office of Becker & Poliakoff, who has represented condos and HOAs for more than 15 years.

“When an owner is asking to install, that’s obviously in condos,” she adds. “In HOAs, nobody cares if an owner wants to do that.

“The law was also expanded to say that if an association wants to install an EV charging station, it doesn’t have to go through the process required for a vote for a material alteration,” states Biletnikoff. “The legislature is encouraging their installation. So that will give boards more freedom to install EV charging stations without having to worry about getting an owner vote.”

Illinois also allows boards leeway in such installations. “Illinois passed legislation on this recently, but it applies only to new-construction HOAs, condos, co-ops, and townhomes, not to the existing market,” reports Sima L. Kirsch, a principal at the Law Office of Sima L. Kirsch P.C. in Chicago, who specializes in representing small to medium condo associations and serves as a mediator for condo disputes.

“On the small-condo side, they’re not installing EV charging stations for the condo – not one of my clients,” she states. “It seems like since the pandemic, especially for smaller condo associations, people are really tightening their pocketbooks.

“Also, if it’s seen as a modification to a system, which the board has leeway on approving, they can do it without owner’s approval,” says Kirsch. “That’s a difficult analysis to go through and to present to the association as to why the board is making the decision. But as we see the trend toward EVs, if there’s an outcry for it in an association, the board will have to consider it.”

CAI Northern Ohio Chapter



Owners will likely need to weigh in if a Virginia community considers EV charging stations. “If you install an addition, alteration, or improvement of more than X amount – some documents say more than \$5,000, some say 1 percent of the annual assessment, some say 5 percent – you must get a vote of the whole community to approve the expense,” explains Molly Peacock, counsel at Rees Broome in Tysons Corner, Virginia, who has represented condos and HOAs for 17 years.

“If the board feels motivated to install EV charges, I think this would qualify,” she adds. “That could trigger a community vote obligation depending on the documents. But I also think it would have a good chance of flying. The uphill battle aspect is that it’s universally difficult to get something approved by owners.

“If the board needs only a majority of the quorum at a meeting, good,” says Peacock. “If it needs a majority of everybody, the chances of success plummet. People are generally accepting of, not clamoring to have, EV charging stations. It’s not like everyone’s dying to have these, but I also haven’t come across opposition.”

Paying for the Upgrades

Stephen T. Brindle, a San Francisco-based senior associate at Swendelson & Gottlieb, a law firm that represents associations throughout California, says he mostly sees individuals installing EV charging stations at the communities he represents. “But I did one recently for a community that wanted to install EV charging stations for the use of all owners,” he recalls.

“The ones I’ve seen have done it on their own because they were going to get a 100 percent rebate,” says Brindle. “In one case, the rebate was about \$300,000, but the board assigned the rebate they were going to receive to the contractor. So the installation was essentially free for the association.”

In that case, the rebate came from the Los Angeles Department of Water and Power, which is the city’s main utility. “That’s the only incentive I’ve seen so far, says Brindle. “The association would sign a contract with the contractor that essentially says ‘We the association assign you to whatever rebate we get, not to exceed \$300,000.’”

Cost is a big concern for Biletnikoff’s clients. “What happens if the electrical transformers can’t support all owners’ doing an individual installation?” she asks. “One of the costs we still don’t know is what happens if you have to upgrade the electrical system to allow the owners to install. Who pays?

“I’m not aware of any incentives being offered by any entity for installing them,” says Biletnikoff. “But one of the innovative solutions one of the lawyers I work with came up with was for boards to say ‘If we install charging stations that are common for the community, maybe it will delay owners from asking for their own and having owners asking to jump that hurdle.’

“And there are companies out there, that for a percentage of the cost you impose for the electric charge, will install and provide the equipment for free,” she says. “I’ve seen a lot of boards use a program where they’re not actually paying the costs.”

CAI Northern Ohio Chapter



Peacock also says her clients are seeing individual owners install EV charging stations, with few associations doing it for the community. “It’s a handful who have them on their property for everybody to use, and it spans both condos and HOAs” she says. “As far as I know for the communities that have installed them, it’s been under \$20,000.”

“The HOA I’m thinking of is made of attached townhomes,” states Peacock. “Sometimes, communities have parking challenges, but in that townhome community, there’s abundant parking. The key is communication with the community. With another client that’s a condo, installation has caused a lot of disputes and lawsuits. One owner wanted to install in their parking space and thought he had more rights than he did. That kind of blew up.”

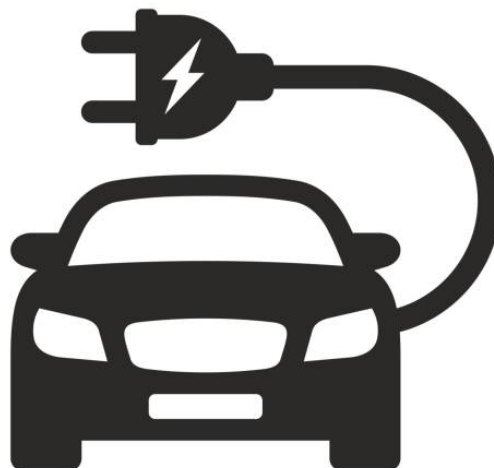
Can You Make Money Off the Equipment?

Peacock says none of her clients are interested in or trying to use EV charging stations to earn income for the community, though that might be possible. “I’d have to look at all the specifics of those condo documents,” she says. “But as long as the money is going back to the association, probably it’s OK.”

In Florida, the question of making a profit might trigger an issue with whether your community is selling energy, which is regulated. “That question always does come up,” says Biletnikoff. “There are associations installing not charging stations but outlets where you can plug your battery in to charge. Can they charge for that? Yes. They can charge for the use of the electricity, but they have to be careful – that profit they might make might mean they’re becoming an electrical provider, which is regulated.”

Brindle also has concerns about profitmaking. “As a general matter, community associations in California are nonprofits,” he explains. “By law, they can levy only as much in assessments and fees as they need to defray their costs. So if there were to start to make a profit off it, that could call into question their nonprofit status.”

“Among my clients, they generally say that anyone who uses the station signs up in advance, and then the association monitors usage and bills costs back to those people,” he adds. “I did have one community in San Francisco that proposed to open their charging station to nonresidents. But once you have your building open to the public, you have to have it Americans with Disabilities Act-accessible. Then you have access issues.”





CAI Northern Ohio Chapter

“Nightmare” Neighbor’s Conviction Gives Condo Owners Relief

Reprinted from the 2021 Exclusive Special Report from *Community Association Management Insider*

Dealing with disruptive residents ranks high on the list of thorny problems community associations — and their management companies — can encounter. You’ve probably heard your fair share of complaints about people violating parking rules or failing to clean up after their pets, but you’ve hopefully never dealt with anything close to the multi-year reign of terror conducted by a condo owner in Orlando, Florida.

If you ever do, we have some advice on how to handle the situation.

Tales of Torment

Marianna Seachrist was a member of the Phillips Bay Condominium Association. In June 2016, the association filed a petition against her with a state arbitrator, alleging that she violated the association’s governing documents in numerous ways and was a nuisance in her condo.

Several witnesses testified on behalf of the association, sharing what the arbitrator dubbed “shocking stories of ... torment.”

For example, after a new neighbor moved in below her unit, Seachrist began loudly playing the movie “The Nightmare Before Christmas” on a continuous loop over the bedroom of the neighbor’s daughter (something the arbitrator, a self-described fan of the movie, labeled “the epitome of a nuisance and malicious behavior”). She also played language lessons very loudly over the neighbor’s bedroom. Seachrist would turn these on and then leave home.

The community association manager testified that she constantly sent him and his company emails accusing them of extorting money from her, engaging in fraudulent activity, and harassing her. Her emails often addressed bushes on common elements that she believed needed to be trimmed. Eventually, she cut these bushes all the way to the ground, requiring removal by the association at its expense.

Seachrist also accused board members of being corrupt, abusing their power, and engaging in vandalism. She threatened to hire someone to kill the association vice president.

The association manager testified as well about the complaints he received from other residents about Seachrist, many of them related to noise coming from her unit. An elderly neighbor wept at an association meeting as she told of the constant pounding noises coming from Seachrist’s unit at all hours. She eventually moved to a hotel and sold her unit because of the noise — and she wasn’t the only resident to leave the community for this reason.

How bad did the noise get? Let’s put it this way: Noise complaints led to multiple arrests of Seachrist. According to news reports, in fact, police visited her condo at least eight times.

CAI Northern Ohio Chapter



On one such visit, they found three low-frequency, “Butt-Kicker” speakers in her unit, connected to an amplifier and held face-down on the floor by dumbbell weights and cinder blocks. The amplifier was attached to a tablet computer playing a “workout mp3” on a loop, and she could turn the tablet on remotely. (Seachrist claimed that she installed the system to fend off insects.)

But wait — there’s more. The cops found video footage of Seachrist stomping around her unit in high-heel shoes and intentionally throwing dumbbells on her floor.

We could go on, with more details of her harassment of other residents (like the one who testified she lived in “constant fear”) and vendors such as landscapers and roofers, but you get the gist.

A Welcome Resolution

Although the arbitrator came down on the association’s side, it didn’t seem to have much effect on Seachrist’s behavior. Nor did the temporary injunction her downstairs neighbor obtained against her in 2015 for stalking protection; indeed, the police were called to her unit about noise for three consecutive days after the injunction was issued. She was arrested, but the charges apparently were dismissed at that time.

At long last, though, the Phillips Bay neighborhood can breathe a sigh of relief. This past February, Seachrist was convicted on charges of stalking and aggravated stalking after an injunction charges, and news reports say she faces foreclosure on her condo.

Tips for Handling Obstreperous Owners

You wouldn’t wish this long, noisy, and stressful process on anyone, but the association generally took the right route to deal with its troublesome (and no doubt troubled) member. Rather than letting their emotions and her provocative activities get the best of them, they consulted legal counsel and filed police reports, pursuing both civil and criminal remedies.

It’s discouraging — but, unfortunately, not unusual — that it took so long to get relief. “One of the difficulties that associations face is that you don’t typically have all these incidents happening at one time,” says Richard Ekimoto, a nationally recognized community association lawyer with the Honolulu firm Ekimoto & Morris, LLC.

Worse, associations can run into arbitrators or judges who feel that board members and management companies should expect a certain amount of harassment by residents. “The law also tends to encourage increasing levels of penalties,” Ekimoto says.

“You don’t just start with legal action, but first try a warning, then fines, and finally legal action.” Even though it may seem obvious that some of the more mild initial steps won’t make any difference, you need to take them, especially if they’re spelled out in the governing documents.

“Sending a letter to a person who is violating the documents, and otherwise engaging in anti-social and nuisance behavior, and expecting a rational response and compliance is unreasonable and unproductive,” acknowledges Ellen Hirsch de Haan of the Tampa, Fla., law firm Wetherington Hamilton. “However, notice and due process must be observed before taking advantage of any of the other remedies available.”

CAI Northern Ohio Chapter



Often, though, the docs lack clear processes for dealing with violations. “If this is the first time a community board is dealing with a significant problem, they may realize their hearing procedures or fine schedule are inadequate or nonexistent,” says Marlyn Hawkins, a partner with the Seattle law firm Barker Martin, P.S.

“It may seem absurd that it took years for Seachrist’s community to get justice, but months can easily fly by if a community feels uncomfortable making an enforcement decision, or if it needs to create or refine procedures for enforcement, or update a fine schedule,” she says. “The best possible way to deal with an enforcement issue is to be proactive by addressing the procedural issues before you need them.”

And when criminal or threatening behavior occurs? “Residents should call the police if they feel threatened, or if they are being harassed or stalked, or other-wise feel their safety is in jeopardy,” de Haan says.

Hawkins agrees. “Ultimately, it’s healthy to acknowledge that your HOA is not the vehicle for solving all of the world’s problems.”



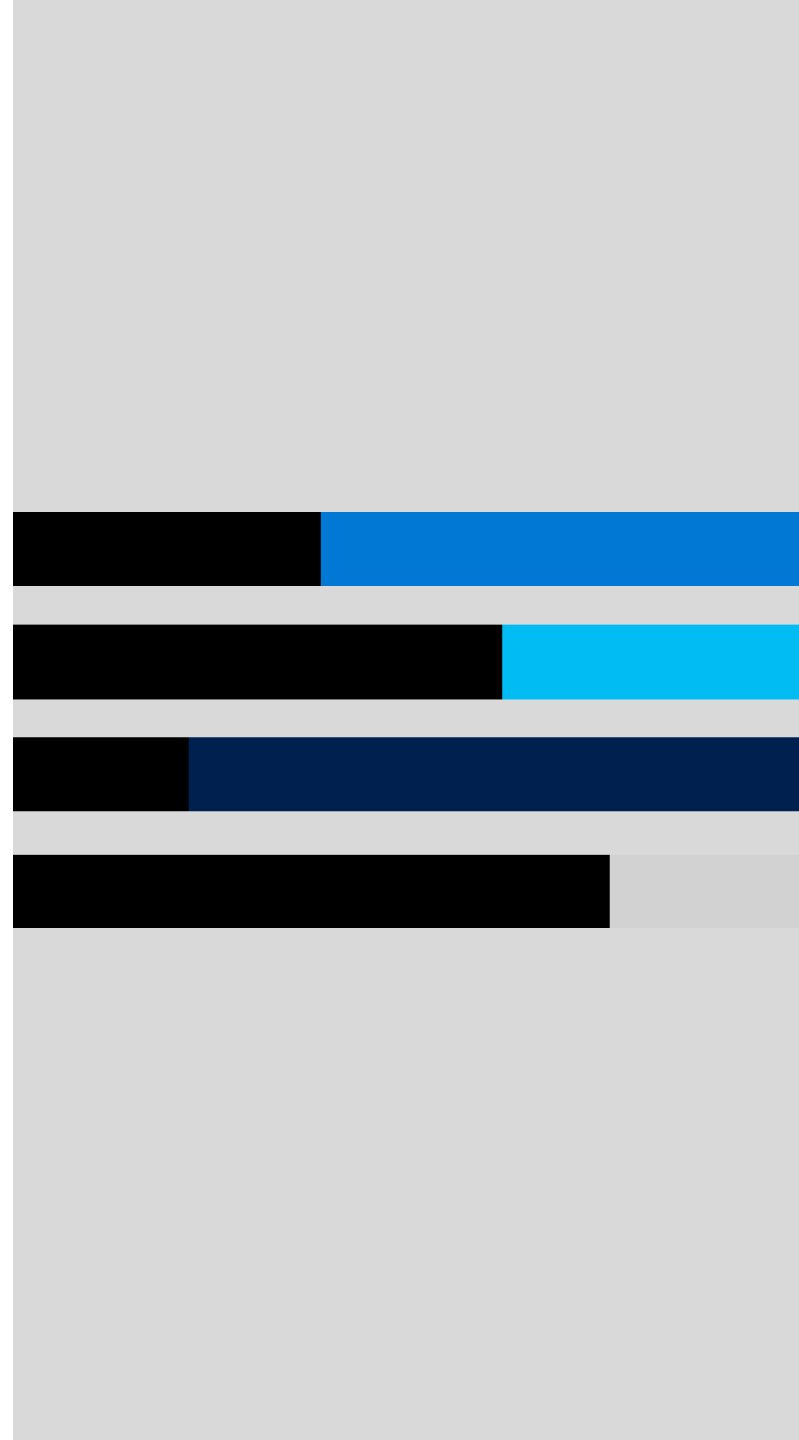
ACC=LLIS

Cybersecurity Training Security & Culture

4/14/2023

00

- | Introduction
- | Know your enemy
- | Creating a cybersecurity culture
- | Cyber threat examples and
- | Miscellaneous Tips



01

| Introduction

| Know your enemy

| Creating a cybersecurity culture

| Cyber threat examples and mitigation

| Miscellaneous Tips



Who is **Accellis**?

- Legendary service, the industry's best tools and education, 25+ industry awards including Best Tech Services Company, and experience unlike any other. Place your trust in Accellis to gain an intelligent edge powered by the Microsoft Cloud and secured around the clock.



Your Cybersecurity partners.

Dedicated internal security team with certifications including Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP). We even built our own Security Operations Center (AgileBlue) and are a proven MSSP.



Why is a Security-Focused culture **important** for your Firm?

A security posture must be built on internationally-recognized standards which is scalable.



Visibility



Business
Reputation



Financial



Trust



Ethics



Protect PII

What is **PII** vs. **Sensitive PII** vs. **PHI**?



PII is a broad term that refers to data that contains the name of an individual plus 1 or more pieces of information that can be used to identify an individual. This could be an address with a name, or an address and a name.

When the **PII** is combined with a birthdate, mother's maiden name, SSN#, driver's license number, etc., it becomes **Sensitive PII**

PHI also contains any type of medical information about the person.

02

| Introduction

| **Know your enemy**

| Creating a cybersecurity culture

| Cyber threat examples and mitigation

| Miscellaneous Tips



Know your enemy!

Conduct a cyber risk assessment

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— **Sun Tzu,**



Types of attackers.

Phishing is a type of cyber attack where an attacker uses deceptive tactics, such as fake emails or websites, to trick individuals into providing sensitive information such as passwords, credit card details, or other personal information.

- Hackers
- Malware Developers
- Insiders
- Social Engineers
- State-sponsored attackers
- Cybercriminals
- Script kiddies
- Hacktivists

But there's one more...

Your worst Enemy: Paper plate guy.

The biggest challenge you have is paper plate guy.



Common ways attackers make it in: Phishing.

Phishing is a cyber-attack where an attacker uses deceptive tactics, such as fake emails or websites, to trick individuals into providing sensitive information such as passwords, credit card details, or other personal information.

- Phishing Types:
 - **"Spear"** targeting specific groups - usually sent from a trusted sender (an already compromised account)
 - **"Whaling"** – Going after accounts of c-level individuals
 - **"Smishing"** and **"Vishing"** phone and text phishing

Common ways attackers make it in : Malware.

A malware attack is an attempt by cybercriminals to infect a computer or network with malicious software, commonly called "malware." Malware is any program or code designed to cause harm, steal data, or gain unauthorized access to a computer system.

- Could come from downloaded software from a forum or blog post
- Drive by from a nefarious website or even search engine
- Unpatched systems with a known vulnerability (zero-day)

Common payload: Ransomware.

Ransomware infects and encrypts files (and sometimes entire disks) to prevent access until a ransom is paid—and there's no guarantee victims will regain access.

- New Ransomware Trends:
 - Focus on data extortion (NVIDIA/Rockstar Games)
 - Data monetization (selling secrets to competitors)
 - Targeting cloud endpoints (crypto mining and botnets)
 - Scaling through Automation (ironically some using blockchain and AI)
 - Exploiting Zero day (easier with automation)



WannaCrypt

May 2017

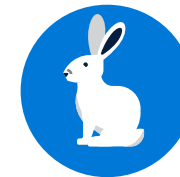
WannaCrypt infects over 230,000 computers — the largest ransomware attack at that time.



SamSam

March 2018

A variant of SamSam malware takes down the City of Atlanta. A ransom of \$51,000 was demanded. Refusal to pay, and poor management afterwards caused nearly \$17 million worth of damage and lost revenue by August.



Darkside

May 2021

Colonial Pipeline is shut down; causing gas price surges through the US and supply issues. Hackers are paid \$4.4 Million in ransom

Stories from the Frontline.

Two stories of loss right here in NE Ohio.

- Dealership using PNC Bank as lender (wire fraud)
- Man in the middle attack small company (3 employees)



03

- | Introduction
- | Know your enemy
- | **Creating a cybersecurity culture**
- | Cyber threat examples and mitigation
- | Miscellaneous Tips



Creating a Cybersecurity **CULTURE.**



Have a Plan



Establish Clear
Policies and SOPs



Training



Encourage Strong
Passwords, SSO,
and MFA



Promote
Reporting



Foster
Accountability

Have a **plan**.



Create a **WISP** (Written Information Security Plan) or Overarching Security Policy

- This is NOT a DRBR plan!
- The purpose is to establish a framework for managing information security risks
- Holds people accountable by naming leadership
- Provides a roadmap for identifying and assessing risks
- Sets cadence for:
 - implementing **security controls** and procedures
 - **monitoring** and reviewing the effectiveness of those controls over time


Improving your Cybersecurity Posture!

How?



- The good news!
 - This has already been done for you!
 - <https://www.nist.gov/cyberframework>

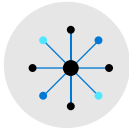
Follow **NIST CSF**.

 NIST (National Institute of Science and Technology) CSF (Cybersecurity Framework)

- A general Framework that can be **tailored** and **scoped** for any size business The purpose is to establish a framework for managing information security risks
- Foundation for HIPAA, CMMC, PCI/DSS



Establish clear **policies and procedures.**



Create an Acceptable Use Policy.



Password policy



Data Usage Policy (including physical) / SOP



▪ Over time:

- Device and data encryption
- Incident Response Plan
- Data/Network Monitoring Policy
- Disaster Recovery/Business Resumption plan
- Tabletop Exercise

Train your staff to limit mistakes.

Why?



Importance of training (Stop Paper Plate Guy!)

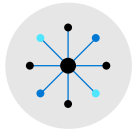
- First line of defense
- Reduce Human Error
- Increase **Awareness**
- Protect Sensitive Data
- Ask the question: Are they protecting their own data?

How?



- Use built-in tools like 365's attack simulation, KnowBe4, Wombat etc.,
- Gameify
- Send to training conferences to keep up with the latest threats
- Online news blogs (knowBe4, Trend, MalwareBytes)

Passwords and user identity .



Use pass phrases. 14 char+ No need to expire!



MFA is **MANDATORY (CONDITIONAL ACCESS)**



Use SSO (Single Sign On) if possible



Use a password manager

| | Lowercase letters only | At least one uppercase letter | At least one uppercase letter +number | At least one uppercase letter +number+symbol |
|----|------------------------|-------------------------------|---------------------------------------|--|
| 1 | Instantly | Instantly | - | - |
| 2 | Instantly | Instantly | Instantly | - |
| 3 | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 1 min | 6 min |
| 8 | Instantly | 22 min | 1 hrs | 8 hrs |
| 9 | 2 min | 19 hrs | 3 days | 3 wks |
| 10 | 1 hrs | 1 mths | 7 mths | 5 yrs |
| 11 | 1 day | 5 yrs | 41 yrs | 400 yrs |
| 12 | 3 wks | 300 yrs | 2,000 yrs | 34,000 yrs |

Encourage **Reporting** and **foster Accountability**.

Why?



Importance of reporting

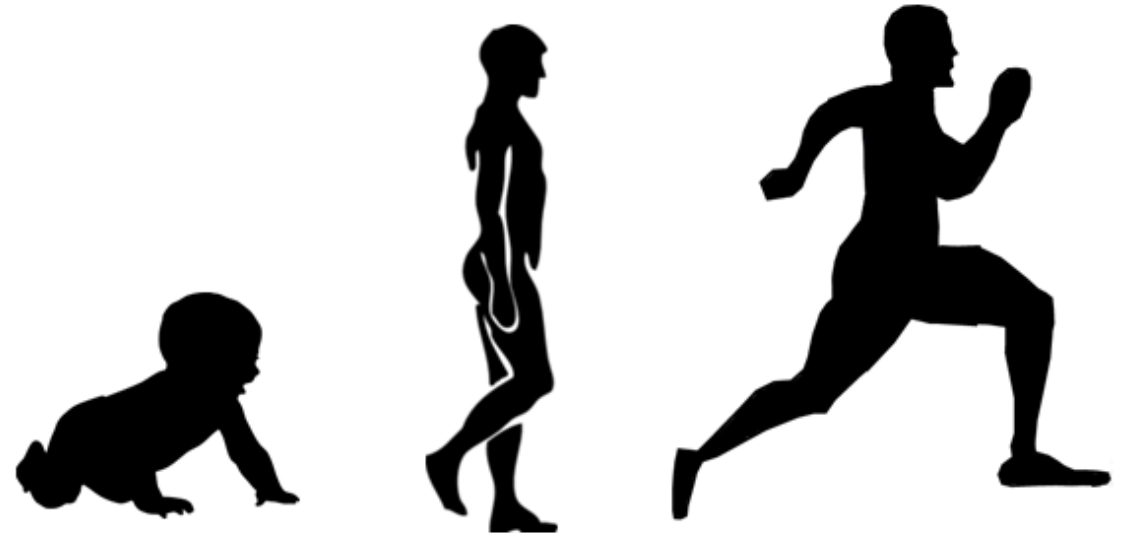
- Could prevent further spread or more harm
- Raise **Awareness** by “Spotlighting” or “Sunshining”
- Learn from past experiences
- Compliance Requirements (reporting leaked data)
- Use culture to spread data ownership and responsibility

Continuous Improvement and **Security Posture.**

How?



- Start with the easy controls (the ones you already have) [Do you use Microsoft 365?](#)
- Budget for cybersecurity initiatives (could be time)
- Implement new controls or improve existing policies and procedures
- Hit the "sweet spot"
- Review controls annually for improvement
- Start assessing your [vendors](#)
- [Saves money on cyber insurance premiums!](#)



04

- | Introduction
- | Know your enemy
- | Creating a cybersecurity culture
- | **Cyber threat examples and mitigation**
- | Miscellaneous Tips



Tips to **identify Phishing**.

How?

- Hovering over links
- Check the Header info
- Misspellings
- Contact your Support Staff (run it up the flagpole)
- Use the Report button in your Antispam Tool

Tips to identify Phishing.

From: Accellis IT Desk <jorgen.akerman@cutnordic.se>
Date: March 13, 2023 at 12:18:05 PM EDT
To: ██████████
Subject: NOTIFICATION NOTICE!: Password Request Maintenance Monday, March 13, 2023



Microsoft Outlook

Hello ██████████

Your (██████████) password is set to expire on N

To avoid account disability or mailbox access restriction
Click below to revalidate credentials

Revalidate Current Password

Accellis.com
IT Support



```
https://api-01.moengage.com/v1/emailclick?em=joaquim.
brites@sma-europe.eu&user_id=@$xy*!hys%c2%b7:
%c3%a7%c3%a8z+ %c3%98□□%c2%b8%c2%9c%c3%8a%c3%9a2%c2%
8e%c2%ae+ %c2%bd%c3%95h%c2%8a%c2%a4a
%c3%b3%00.5&td=@$xy*!hn%c2%8e<`f;$\
or□%c2%97+ %c2%87cm&cid=@$xy*@!
h%c2%ba%c2%a7m%c2%9e%c2%9e□□d%c2%90%c2%bf%c3%aezf□%
c3%b9□%c3%b9%c3%b4b%c2%92!%c2%81□%c2%89rxvm%c2%92v(%
c2%91%c3%91%00%c3%afs%c2%a7%c2%86v%c3%a4?
%c3%91%c2%9bot%c2%b3j%c2%be%c3%87%c2%acvs□%c3%be%c3%
81%c3%91%c2%aaqid%c3%b8%c3%b3□,□+>\
%c3%88%c3%88%c3%97o!□%c2%aa%c3%a1%
%c2%bf%00□&ut=l&moeclickid=61b35f5997223f7c61e6625a_f_t_em_a
b_0_p_0_time_2021-12-10+14:09:02.859891_1_0ecli27&rlink=http://
cczjieeyrn4ckxqvjcbrq.bvesbebbihox2wz85acjj.betil.com.tr?pid/
ymd1c2nvdhraywnjzwxmuy29t
Click or tap to follow link.
```

Tips to **identify Phishing.**

Jeff Thwing

From: Jacob Rockwell <officemai59602@gmail.com>
Sent: Monday, April 3, 2023 1:49 PM
To: Jeff Thwing
Subject: Updating Of Account Information

Hi, I just opened a new bank account, thus I need to change the information for my direct deposit. I need your help now, please. Do I have to fill out a form?

Can the change be made before the next pay period?

Regards.



will you need?

Tips to **identify Phishing.**

From: Admin <luigi.schinner36010@icloud.com>
Date: March 24, 2023 at 6:01:22 PM EDT
To: Brian Guscott <bguscott@accellis.com>
Subject: **Notificatoin Friday, March 24, 2023**



Fax message has been verified by BGuscott@accellis.com safe senders list.





This E-mail was sent from "Canon 5045 Scanner" (IM F5377).

[Review.Fax.Pdf](#)

Queries to: accellis.com

Tips to **identify Phishing.**

 **Jeff Thwing** <JThwing@accellis.com>
To:  Tom Fazio

 **JEFF THWING**
 Business Operations Manager
 216-662-3200 Ext 140


-----Original Message-----
From: Nicholas Marquette <duluxeedition816@gmail.com>
Sent: Thursday, March 9, 2023 9:37 AM
To: Jeff Thwing <JThwing@accellis.com>
Subject: New -DD PAY

Hi Jeff ,
I want to change my direct deposit to a new account. What details will you need?

Regards,
Nicholas Marquette
Project Manager
Accellis Technology Group, Inc.

SOCIAL ENGINEERING TACTICS

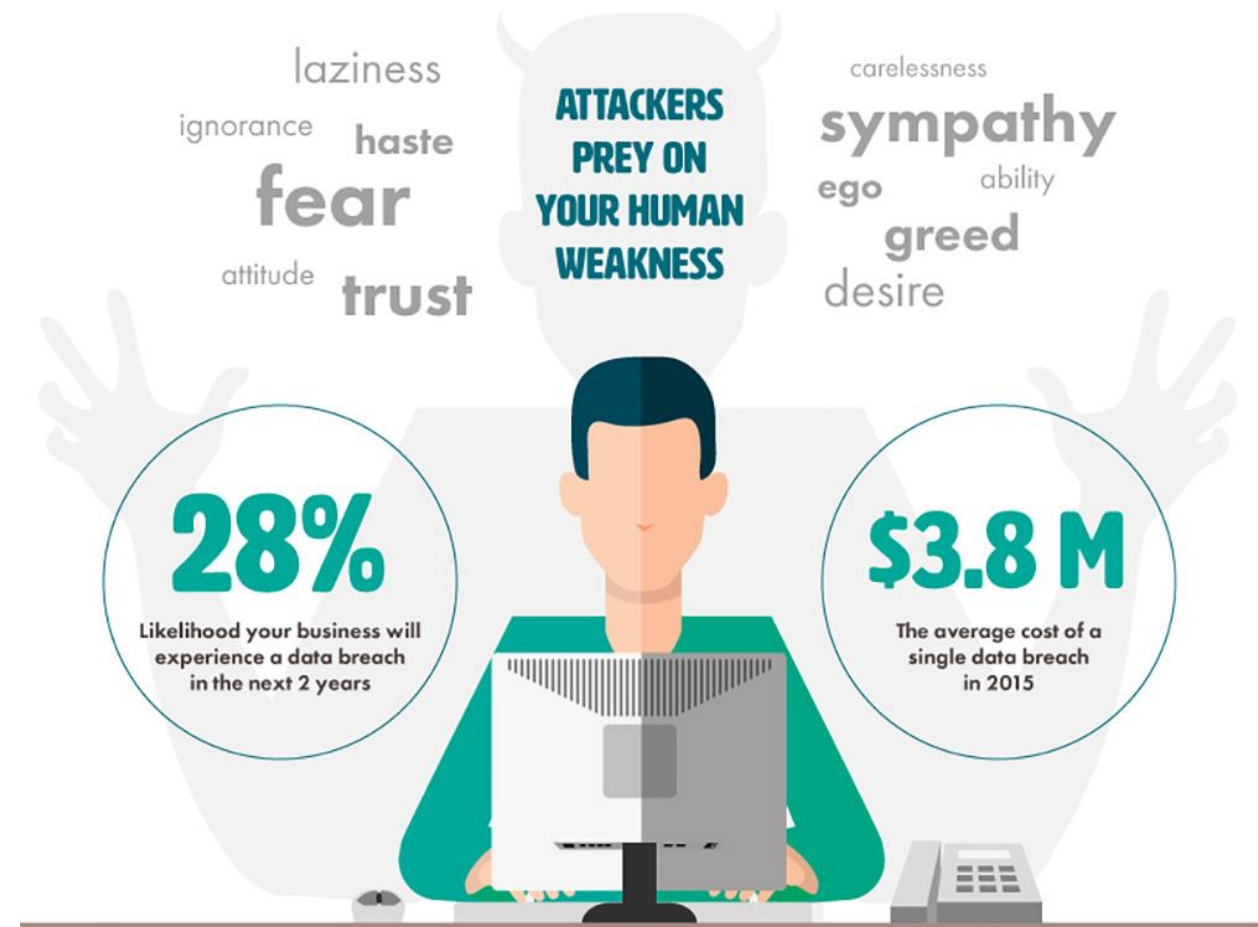
YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERING ATTACKS.

WHY SOCIAL ENGINEERING?

HACKING A HUMAN IS **MUCH EASIER** THAN HACKING A BUSINESS.

Social Engineering

- People are easier to hack than Computers!
- The Attacker's Method:
 - Gather Information
 - Establish Trust or Power
 - Heighten Emotions
 - Time Limits
 - Control the Conversation
- The Attackers Tools:
 - Social Media
 - Email
 - Phones
 - Public record
 - Hi-Vis vest and a clipboard
- Verify Identity
- Do not bypass processes
- Two keys to the Money Vault



05

- | Introduction
- | Know your enemy
- | Creating a cybersecurity culture
- | Cyber threat examples and mitigation
- | **Miscellaneous Tips**



Tips to Secure Social Media

- Do not divulge too much public information
- Don't do personality quizzes!
- Always be on alert – Don't answer that random Facebook Messenger
- Upgrade to a strong, unique password for each account and enable two-factor authentication
- Check your LinkedIn settings (next slides)
- Check your Facebook settings (next slides)

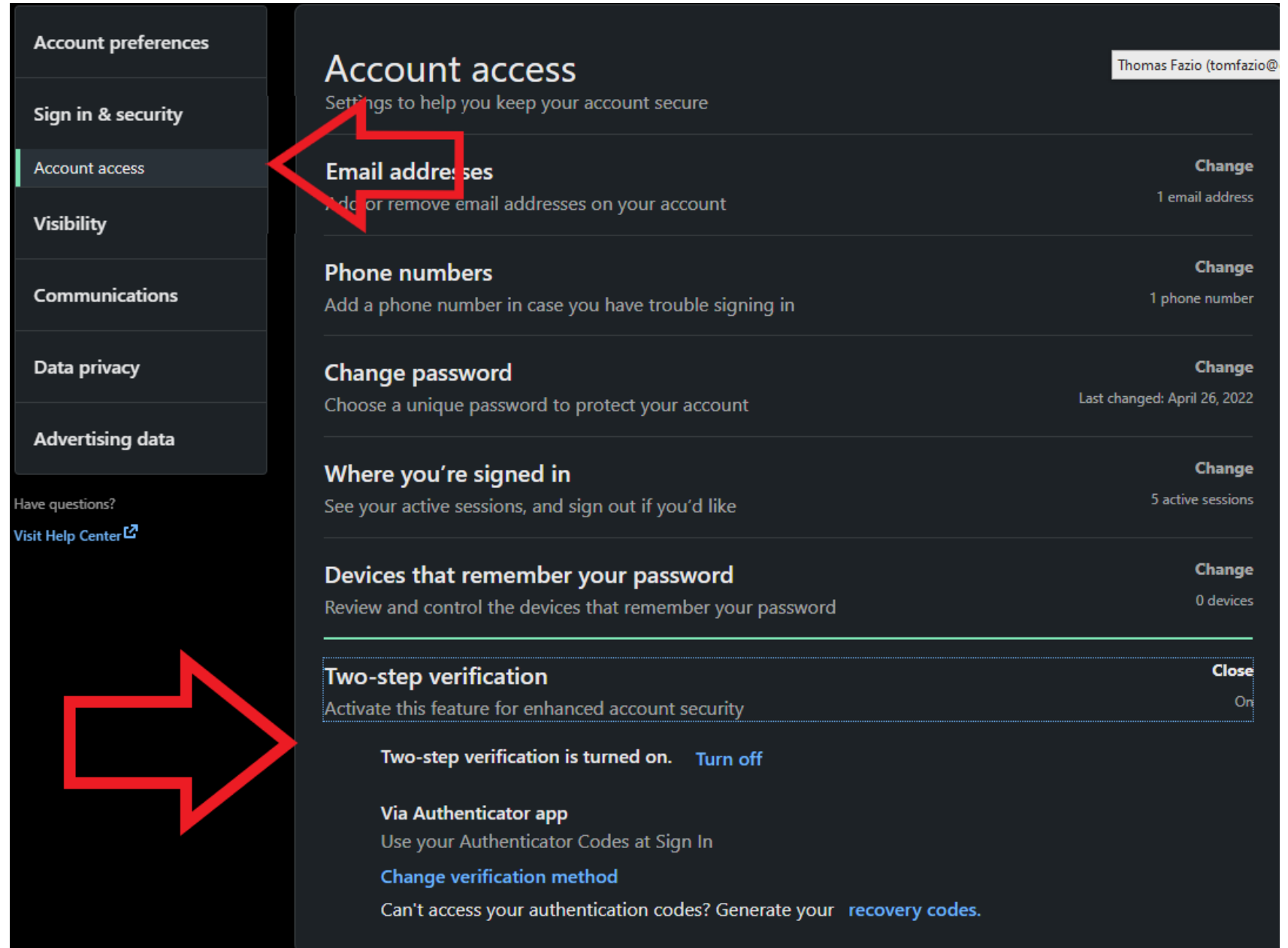
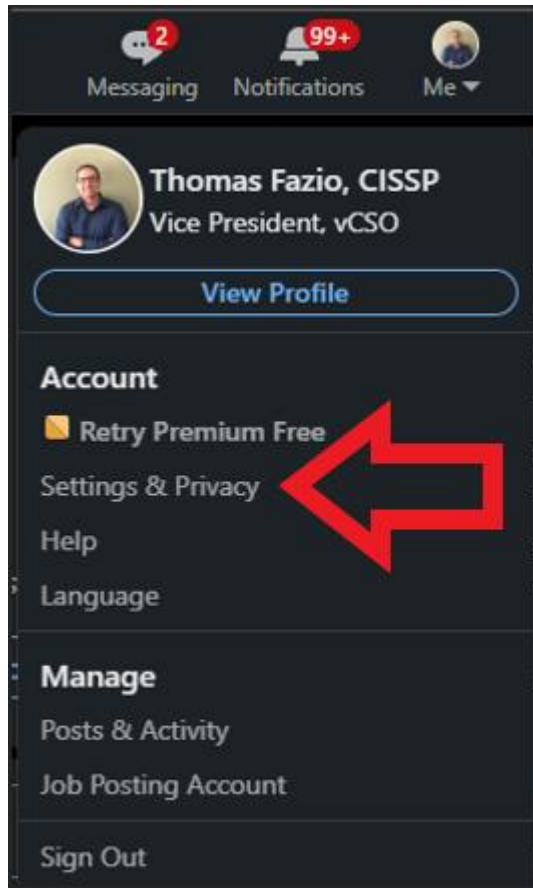


BORED IN ISOLATION?
Let's get to know each other better!

| | |
|--|--------------------|
| First job title: | STOP |
| Favorite Food: | GIVING |
| Favorite Color: | PEOPLE |
| First Pet's Name: | YOUR |
| First Child's Name: | PERSONAL |
| Favorite Restaurant: | INFORMATION |
| Where Are You From: | TO |
| Favorite Singer/Band: | GUESS |
| Mother's Maiden Name: | YOUR |
| First Type of Car: | PASSWORDS |
| First Job: | AND |
| First Met Your Significant Other: | SECURITY |
| High School Mascot: | QUESTIONS |

These games seem like fun, but could have dangerous consequences. Don't fill out these surveys online.

Using Social Media - LinkedIn



Using Social Media – LinkedIn cont.

The image shows a screenshot of the LinkedIn account preferences page. On the left is a navigation menu with the following items: Account preferences, Sign in & security, Visibility, Visibility of your profile & network (highlighted with a green bar), Visibility of your LinkedIn activity, Communications, Data privacy, and Advertising data. Below the menu are links for 'Have questions? Visit Help Center' and a red arrow pointing to the 'Who can see members you follow' section. The main content area is titled 'Visibility of your profile & network' with the subtitle 'Make your profile and contact info only visible to those you choose'. It contains several sections: 'Profile viewing options' (set to Private mode), 'Edit your public profile', 'Who can see or download your email address', 'Connections', and 'Who can see members you follow' (set to Self). The 'Who can see members you follow' section has two radio button options: 'Only visible to me' (selected) and 'Anyone on LinkedIn'. Below this section is explanatory text and a 'Learn more' link. At the bottom, the start of another section 'Who can see your last name' is visible.

Account preferences

- Sign in & security
- Visibility
- Visibility of your profile & network**
- Visibility of your LinkedIn activity
- Communications
- Data privacy
- Advertising data

Have questions?
[Visit Help Center](#)

Visibility of your profile & network

Make your profile and contact info only visible to those you choose

Profile viewing options Change
Choose whether you're visible or viewing in private mode Private mode

Edit your public profile Change
Choose how your profile appears to non-logged in members via search

Who can see or download your email address Change
Choose who can see your email address on your profile or in approved apps or download it in their data export

Connections Change
Choose if your connections can see your connections list No

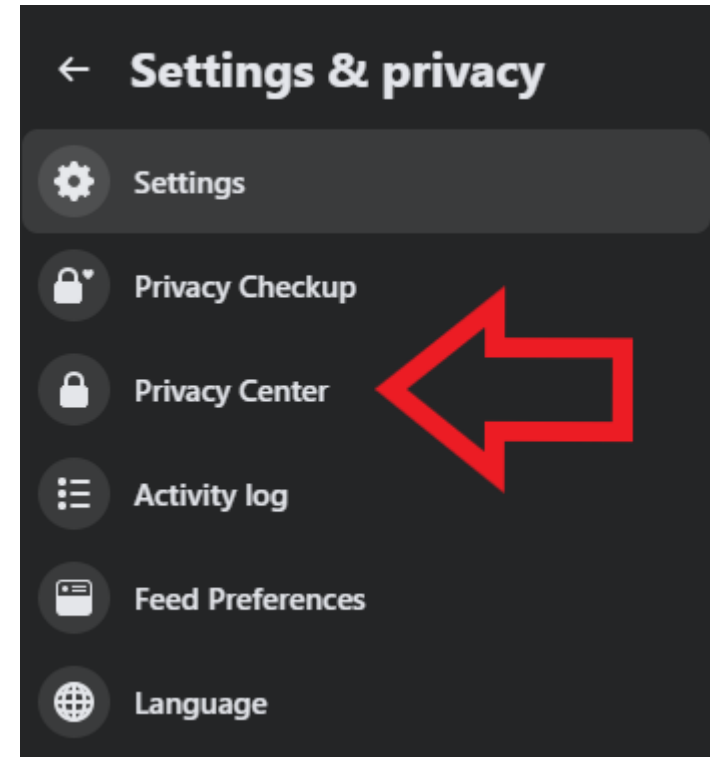
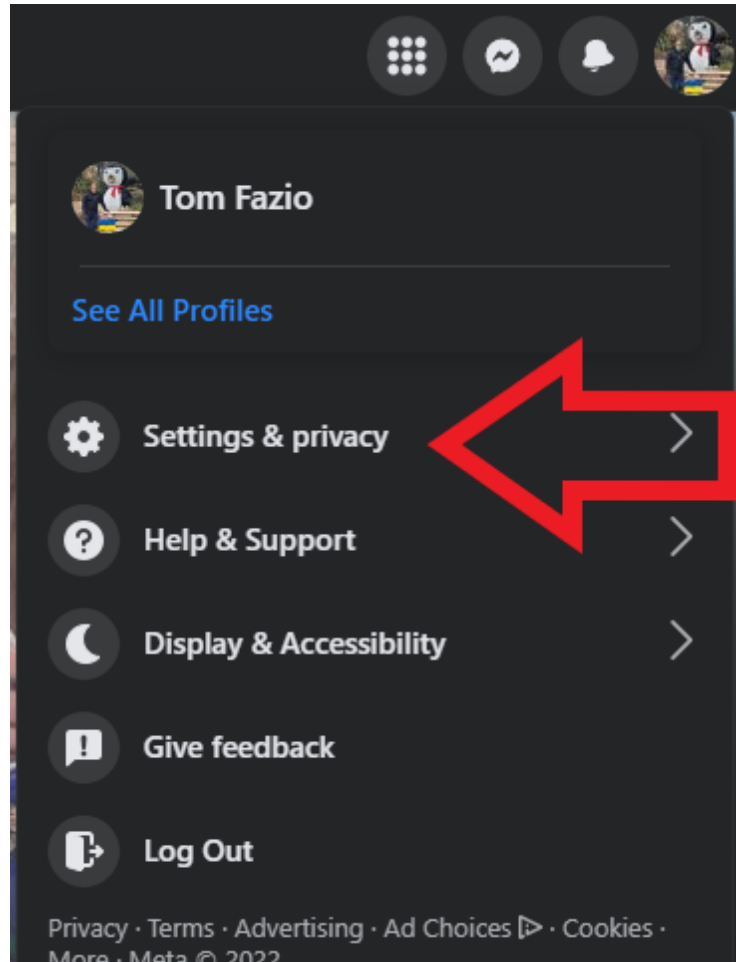
Who can see members you follow Close
Choose if others can see who you follow Self

Only visible to me
 Anyone on LinkedIn

This setting only affects your follow visibility for other members, not for LinkedIn Pages or hashtags. If you follow a member, that member can always see that you follow them. [Learn more](#)

Who can see your last name Change

Using Social Media – Facebook



Using Social Media – Facebook

- Make sure public cannot see friends list

Settings

- General
- Security and login
- Your Facebook information
- Privacy**
- Face Recognition
- Profile and tagging
- Public posts
- Blocking
- Location
- Language and Region
- Stories
- Journalist resources
- Notifications
- Mobile
- Apps and Websites
- Business Integrations
- Ads
- Ads Payments
- Facebook Pay

Privacy Settings and Tools

Privacy shortcuts

- Check a few important settings
- Quickly review some important settings to make sure you're sharing with the people you want.

Manage your profile

Go to your profile to change your profile info privacy, like who can see your birthday or relationships.

Learn more with Privacy Basics

Get answers to common questions with this interactive guide.

Your Activity

| | | |
|---|---------|------------------|
| Who can see your future posts? | Friends | Edit |
| Review all your posts and things you're tagged in | | Use Activity Log |
| Limit the audience for posts you've shared with friends of friends or Public? | | Limit Past Posts |
| Who can see the people, Pages and lists you follow? | Only me | Edit |

How people find and contact you

| | | |
|---|--------------------|------|
| Who can send you friend requests? | Friends of friends | Edit |
| Who can see your friends list? | Only me | Edit |
| Who can look you up using the email address you provided? | Friends | Edit |
| Who can look you up using the phone number you provided? | Friends | Edit |
| Do you want search engines outside of Facebook to link to your profile? | No | Edit |

