

Avoid the Lockout

Social Media Safety for Your Team



RIPPED FROM THE HEADLINES



Associated Press

Elmo's hacked X account posted racist messages. Sesame Workshop is trying to regain control

yahoo/news

<https://www.yahoo.com/news/elmos-hacked-x-account-posted-143021867.html?guccounter=1>

[Sesame Workshop](#) was trying to regain full control over its Elmo account on the X platform Monday after a hacker gained access...

“Elmo’s X account was compromised by an unknown hacker.... We are working to restore full control of the account,” a Sesame Workshop spokesperson said Monday. Sesame Workshop is the nonprofit [behind “Sesame Street”](#) and Elmo.

OUTLINE:



1. Real Story: YouTube Channel Gone
2. Why This Happens
3. Real Consequences
4. BC/DR - The Bigger Picture
5. Domains - The Root of Everything
6. Red Flags to Look For
7. First Steps to Regain Control
8. Build a Safer System
9. Summary & Next Steps
10. Q & A + Resources



Good morning and welcome! My name is James, and I've been working in IT for almost 3 decades. I've held IT Director titles for half of that time. A major part of my responsibilities included overseeing onboarding and offboarding staff, managers, and board members as it related to technology access. In the past three years I have been operating my own business with a focus on website development and hosting, along with supporting productivity suites.

In that time I have worked with many nonprofit organizations, and small to medium sized businesses. Sometimes I think I've seen it all, and then the next day, something new happens. I've been called into work early because there was a weather event that nearly destroyed one offsite office while one of the retail sites lost their fiber Internet service due to fallen trees. Once a car accident took out a transformer behind a retail site, and another time a rodent of some kind chewed through the coaxial cable feeding primary internet and some phones services. It's not too difficult to see that disasters happen, and that it is essential to be prepared for when they happen. Most importantly, I have found through bitter experience that it is even more important to prevent some types of disasters before they happen, and to have mitigation strategies in place if prevent efforts fail.

In the scope of IT, this includes social media accounts. In my experience, they can be the most difficult platforms to protect from a business or organizational perspective. Let's talk about that.

YouTube Channel with 20K Subscribers... Gone.



- Created by staff using personal Gmail
- Grows to 20,000+ subscribers
- Staff leaves, becomes unreachable
- Account inaccessible, unrecoverable
- Forced to start over from scratch



Let's start with a real example. I worked at a charitable nonprofit for just under five years as the IT Director. Before I had started there, they had a staff person who had set up and managed their YouTube channel using a personal Gmail account. Years had passed, and the channel grew in content and subscribers. But when that staff member left, they took the login access with them. The org had no way to recover it. Their videos, comments, subscribers - all stuck behind a wall. We had to start a new channel with the proper controls in place.

This isn't rare. It happens a lot - especially with social media accounts like Facebook (or Meta) business pages, Instagram, LinkedIn, X (formerly Twitter). Facebook is probably the most challenging since you have to have a personal Facebook account to create and manage a Facebook business page.

Why So Many Teams Lose Access



- Shared passwords with no master list
- Platforms tied to personal emails
- No onboarding/offboarding process
- Unclear ownership/responsibility



This happens because many small teams rely on shared passwords, or they don't know who set what up. It's ad-hoc and informal. That works fine - until someone leaves or a crisis hits.

What Can Go Wrong



- Lost visibility & engagement
- Reputation damage
- Confusion across platforms
- Former staff can still access accounts



The fallout is real: your org can't reply to messages, post updates, or protect your branding. And worse - you don't know what the former staff might do with those accounts.

Basic Business Continuity & Disaster Recovery (BC/DR)



- **Business Continuity (BC)** is about keeping essential business functions running during a disruption.
- **Disaster Recovery (DR)** is about restoring data and systems after a disruption.



Think of this through a business continuity and disaster recovery lens. If a key staff member wins the lottery and quits tomorrow, can your organization still function online? We're sharing these strategies from that mindset - building resilience.

Business Continuity (BC) is about keeping essential business functions running during a disruption.

Disaster Recovery (DR) is about restoring data and systems after a disruption.

Basic Business Continuity & Disaster Recovery (BC/DR)



- **What happens if the one person with access is gone?**
- What's your plan if a platform locks you out?
- Apply BC/DR thinking to social platforms
- The goal: resilience, not just access



Basic Business Continuity & Disaster Recovery (BC/DR): Applied to Social Media Accounts:



- Contact List
- Data Backup
- System Recovery Plan
- Access Plan
- Password & Account Access
- Communication Plan
- Inventory
- Test Schedule



Contact List - Know who has access to each account - staff, contractors, or partners.

Data Backup - Regularly export key posts, ad data, follower lists, and insights (most platforms allow this).

System Recovery Plan - Have a process for regaining access if an account is hacked or someone leaves with login control.

Access Plan - Use shared tools (like Meta Business Suite or a social media manager) to give controlled access—avoid using personal logins.

Password & Account Access - Store logins and recovery emails securely (like in a password manager). Use 2FA tied to a shared, secure phone or email—not someone's personal account.

Communication Plan - Have a backup channel (like email or a second platform) to reach your audience if one account is down.

Inventory - Maintain a list of all platforms in use, login URLs, admin roles, and recovery info.

Test Schedule - Periodically verify that logins work, 2FA is current, and admins are up to date—especially after staffing changes.

Protect Your Domain – Protect Your Identity



- Many orgs don't use branded domains or email
- Domain loss = loss of email, website, and recovery options
- Always enable auto-renew
- Use trusted off-domain email as backup recovery
- Make sure more than one person has registrar access



Your domain is your digital identity. Losing it can be worse than losing a social media account. If you're not using a branded domain for email, you're missing out on control. Also, make sure it auto-renews, and use backup accounts that aren't tied to your own domain - because if the domain is down, so is your email.

Watch Out For These Warning Signs



- No list of who has access
- Logins tied to personal accounts
- Only one person with admin rights
- MFA tied to someone's phone
- No offboarding process



These are the signs you're at risk. If you don't know who has the keys, you probably don't have them all. If the only admin is someone who left last year, that's a problem.

What You Can Do Right Now

- List every platform your org uses
- Check who has access & what level
- Change logins from personal to org-owned
- Turn on 2FA with org-managed backups



Start by auditing what you have. Make a list of accounts, figure out who has access, and begin migrating them to accounts your organization owns and can recover.

Long-Term Protection Practices

- Use role-based email accounts (social@, info@)
- Use a password manager (like LastPass)
- Document logins & share with leadership
- Offboarding checklist for departing staff
- Assign a social media steward



Put systems in place that don't rely on any one person. Use tools built for teams. And most importantly, document your access and have clear policies for when people leave.

Take Back Control Before It's Too Late:

“Take your medicine”

- Audit your accounts today
- Migrate access to org-owned emails
- Use tools to manage logins
- Set policies for continuity

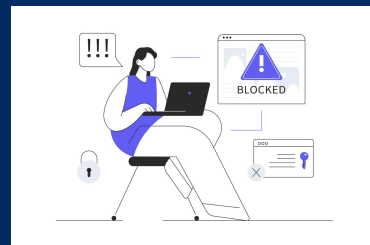


This is about setting your team up for success and safety. The steps are simple but powerful. Don't wait until something breaks. Start now.

What if it's too late?



- Try logging in from all known devices
- Check for other admins who can restore your access
- Visit the platform's account recovery or help center
- Report the issue if the account was hacked or ownership changed
- Submit business documentation if needed to prove ownership
- Secure related accounts (email, phone number, password manager)
- Review and update your access and recovery procedures afterward



Specifically for Facebook:

Check Business Manager Access – Log into [Meta Business Suite](#) and see if you still have page access.

Identify Other Admins – Ask another page admin (if any) to restore your role.

Check Your Profile – Make sure your personal profile is still active and not restricted or hacked.

Use Facebook's Help Form – Go to [Facebook's Business Help](#) and use the "Get Help" option or access the [Page Admin Dispute Form](#) if needed.

Report a Compromised Account – If you believe your personal Facebook account was hacked, report it here: facebook.com/hacked.

Appeal Page Ownership – If ownership was wrongly taken or changed, submit a claim with business documentation (business license, domain ownership, etc.).

Resource: Social Media Access Safety Checklist

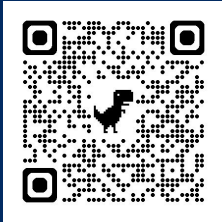
- ❑ Create a centralized list of all social media platforms used by your org
- ❑ Identify who has access and what level (Admin, Editor, etc.)
- ❑ Migrate accounts from personal to org-owned email addresses
- ❑ Set up role-based email accounts for platform ownership (e.g., social@yourorg.org)
- ❑ Turn on two-factor authentication (2FA) for all accounts
- ❑ Use a team password manager (e.g., Bitwarden, LastPass)
- ❑ Document all recovery methods (email, phone, backup codes)
- ❑ Confirm multiple staff have admin access to each platform
- ❑ Ensure domain is set to auto-renew with alerts in place
- ❑ Use at least one off-domain recovery email for registrar login
- ❑ Review and update access quarterly
- ❑ Create an offboarding checklist that includes access revocation
- ❑ Assign ongoing responsibility for monitoring account access

AVOID THE LOCKOUT



QUESTIONS?

THANK YOU!



 **Erawatech**