Post-Compromised Account Cleanup Guide

This guide is for Mercer County Community College Employees and Students whose accounts were recently compromised via a phishing attack and have now been reset and re-enabled. **Please follow all steps immediately** to secure your account and check for malicious activity.

Phase 1: Immediate Account Security Checks

The first step is to ensure the scammer has not left a backdoor or way to regain access.

A. Change Your Password (Again)

- Even if IT has reset it, choose a **new, strong, unique password or passphrase** right now. This is your primary defense.
- **For Students or Employees Without College Laptops/Computers:**
  Link: https://mysignins.microsoft.com/security-info/password/change

- **For Employees with College Laptops/Computers (On-Campus or VPN):**
  1. On your college-issued laptop or computer, while on campus or on VPN, press **CTRL+ALT+DEL** simultaneously on your keyboard.
  2. Select the **Change a password** option.
  3. Enter your Old password, then enter your new password and confirm it.
  4. Allow up to two hours for the new password to synchronize across all college applications and services. During this synchronization period, you may need to try your old password or your new password to log into different applications until the process is complete.

B. Check and Re-establish Multi-Factor Authentication (MFA)

- Verify that your MFA device, phone number, email addresses, or application is the only one registered. Remove any unrecognized devices.
- **Action:** Go to your **My Sign-ins** page and click **Security Info**.
- **Link:** https://mysignins.microsoft.com/security-info

C. Review Email Forwarding Rules

- Scammers often create a hidden rule to forward your emails. Delete any rules you did not create, especially those forwarding emails to external domains (e.g., Gmail, Yahoo).
- **Action:** Go to your **Outlook Settings** >> **Mail** >> **Rules** and **Forwarding**.
- **Link:** https://outlook.office.com/mail/options/mail/rules

D. Check for Suspicious Delegates/Permissions

- Ensure no one has been given delegate access to send emails on your behalf or manage your calendar. Remove any unfamiliar names.
- **Action:** Go to **Outlook Settings** >> **Mail** >> **Shared Mailboxes/Delegation**.
- **Link:** https://outlook.office.com/mail/options/mail/delegates

E. Ensure your direct deposit has not changed

- **If you are an employee**, check that your bank account number has not changed. Scammers will attempt to redirect your paycheck to other third-party scammers.
- **Action:** Go to **Self-Service >> Employee >> Banking Information**
- **Link:** https://mercer-ss.colleague.elluciancloud.com/Student/HumanResources/BankingInformation

Phase 2: Finding and Removing Malicious Content

Scammers may have used your account to create fake documents and forms, targeting others. It is crucial to locate and remove these items.

A. OneDrive/SharePoint Cleanup (Fake Documents)

- **1. Check Your "Recently Modified" Files**
  - Look for any files or folders you did not create, especially those with suspicious titles. Sort files by **Date Modified** to see recent changes.
  - **Action:** Go to your OneDrive and review recent activity.
  - **Link:** https://mccc0-my.sharepoint.com/
- **2. Check Your "Shared" Files**
  - The scammer may have shared malicious files from your account. Look for and **unshare any suspicious documents, then delete them**.
  - **Action:** Go to the **Shared** section of your OneDrive.
  - **Link:** https://mccc0-my.sharepoint.com/?v=ShareBy
- **3. Review Your Recycle Bin**
  - The scammer might have tried to hide evidence by deleting items. Check the bin for suspicious documents.
  - **Action:** Go to the **Recycle Bin** on your OneDrive. Delete anything you do not recognize.
  - **Link:** https://mccc0-my.sharepoint.com/?v=recyclebin

B. Microsoft Forms Cleanup (Fake Forms/Surveys)

- **1. Review All Forms You Own**
  - Scammers create a new form using your account to steal credentials or sensitive data. Look for any forms you do not recognize.
  - **Crucial Step:** If you find a malicious form, **DO NOT OPEN** any responses. Delete the form **immediately**.
  - **Link:** https://forms.office.com/

Phase 3: Protecting Yourself Outside of the College (Personal Security)

This section is dedicated to securing your personal accounts and identity, as the MCCC security team is only responsible for the integrity of your college accounts.

If your MCCC login information was also used for any personal accounts (a practice we strongly advise against) or if you suspect identity theft, **immediate personal action is required.**

A. Immediate Personal Account Security Actions

1. **Change Personal Passwords:**
   - Immediately change the password for any personal account that used the **same or a similar password** as your compromised MCCC account (e.g., personal email, banking, social media).
   - **Crucially, use a unique and strong password** for every single personal account. Never reuse passwords.
2. **Review Personal Email Accounts:**
   - Log in to your personal email accounts (Gmail, Outlook, Yahoo, etc.).
   - Check for any suspicious login notifications or account changes you didn't authorize.
   - Review the email settings for new, unfamiliar **Forwarding Rules** or **Mailbox Delegates** (just as you did in Phase 1 for your MCCC email). **Delete any suspicious settings immediately.**

B. Official U.S. Government Resources

If you suspect financial compromise, identity theft, or need further guidance on securing your personal life, we strongly encourage you to consult the official U.S. government resources provided below:

- **IdentityTheft.gov (Federal Trade Commission - FTC)**
  - This is the U.S. government's official resource for identity theft. It helps you report identity theft and creates a personalized recovery plan, complete with a checklist and sample letters to send to businesses.
  - **Link:** https://www.identitytheft.gov/
- **Consumer.gov (Federal Trade Commission - FTC)**
  - Provides consumer advice on topics like identity theft, credit freezes, and general tips for staying safe online.
  - **Link:** https://consumer.ftc.gov/identity-theft-and-online-security/identity-theft
- **Social Security Administration (SSA)**
  - Offers guidance on checking your earnings history and securing your Social Security Number (SSN) against fraud.
  - **Link:** https://www.ssa.gov/fraud/

C. Report to Law Enforcement

If you have completed your FTC report and can provide proof of financial loss or fraud (e.g., a bank statement, credit card charge), **you may need to file a report with your local police department.**

- Call the non-emergency line of your local police department.
- Bring a copy of the recovery plan/report created on **IdentityTheft.gov** to the police station.

Phase 4: Communicate and Report

1. **Notify Your Contacts:** Send the prepared warning email to all people you've been in recent contact with, stating your account was compromised, and they must delete any recent links or forms from you.
2. **Report Remaining Suspicious Activity:** If you find any settings, files, or forwarding rules you cannot delete or don't understand, **notify the Help Desk at https://mitts.mccc.edu immediately**.

Here is a draft of the email that you should send to your contacts (both internal and external) immediately after completing the security steps. This draft is designed to be professional, urgent, and focused on protecting the recipient.

📧 Draft Email: Compromised Account Warning

Employees should customize the highlighted sections before sending.

Subject: ⚠️ URGENT: My Account Was Compromised — Please Delete Recent Emails/Links

Dear colleagues and contacts,

I am writing to inform you that my email account was recently compromised by a phishing scam. The issue has been contained, and my account is now secured and monitored by our IT team.

Action Required from You:

- **Immediately delete** any emails, OneDrive links, or Microsoft Forms/Surveys you received from me between **[Start Date/Time]** and **[End Date/Time]**.
- **Do not click on any links, open any attachments, or fill out any forms** sent from my account during that period. These may contain malicious links or be attempts to steal your information.

If you clicked on any links or provided information via a form from my account during this time, please notify your own IT security department immediately. At MCCC, you can notify MITTS at https://mitts.mccc.edu.

I sincerely apologize for any disruption or concern this may cause.

Thank you for your immediate cooperation.

Sincerely,

[Your Name]