Steps to take if you have been phished

If you've given out your information to a phisher, it's important to act quickly to minimize potential damage. Here are the steps you should take:

1. **Change Your Passwords**:
    - Immediately change the passwords for any accounts that might be compromised. Use strong, unique passwords for each account.
2. **Enable Two-Factor Authentication (2FA)**:
    - Enable 2FA, if available on your accounts, to add an extra layer of security.
3. **Report the Incident**:
    - Report on the phishing attempt to the IT department. They can provide additional support and may take steps to protect other students and staff.
    - You can also report the incident to the Federal Trade Commission (FTC) or your email provider.
4. **Report and Block Spam Text Messages:**
    - Report Spam Texts to Your Carrier by forwarding spam text message to 7726 (SPAM). This is a common short code used by many carriers to report spam texts.
    - Block numbers manually by tapping on the number or contact and select block or report as spam.
5. **Monitor Your Accounts**:
    - Keep a close eye on your bank accounts, credit card statements, and other college-related accounts for any suspicious activity.
6. **Contact Your Bank or Credit Card Company**:
    - If you provided financial information, notify your bank or credit card company. They can help you monitor fraudulent activity and may issue new cards.
7. **Check Your Email Settings**:
    - Ensure that no unauthorized changes have been made to your email settings, such as forwarding rules or recovery email addresses by visiting the Google security checkup page using this link. https://myaccount.google.com/intro/security-checkup?hl=en-US

8. **Consider a Credit Freeze or Fraud Alert**:
    - If you are a victim of identity theft, you have the right to file a police report and are permitted under Massachusetts law to place a security freeze on your credit reports.
    - If you provided sensitive information like your Social Security number, consider placing a credit freeze or fraud alert on your credit reports to prevent new accounts from being opened in your name.
    - Use these links to find more information from the three credit bureaus.
        - TransUnion
        - Equifax
        - Experian
9. **Educate Yourself:**
    - **S**tay informed about the latest phishing tactics and how to recognize them.

Taking these steps can help protect your personal information and reduce the risk of identity theft.