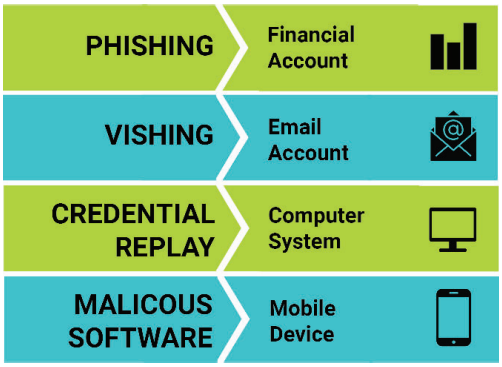
Cyber Crime Fraud Protection

One Step Ahead: Protect Yourself Against Cyber Crime

In an era where cyber criminals employ increasingly sophisticated tactics, safeguarding your information is more crucial than ever. Threats range from deceptive websites and AI-driven voice cloning to fraudulent QR codes and conventional phishing attempts via email, calls, or texts.

Cyber criminals operating today apply a number of tactics to achieve their goals. Still, most cyberattacks share commonalities in their objectives and execution. Attacks typically use one or more of the most common methods of circumventing your security – known as attack vectors – in order to compromise financial accounts, email accounts, computer systems, or mobile devices. Once they have control, they will find ways to monetize that access.

Ways of Attack



1) **PHISHING** is a fake electronic message designed to trick you into divulging information and/or providing access that you shouldn't. Typically phishing is used to acquire sensitive data such as financial account information or login credentials. The perpetrator may pretend they are a trusted person or entity and may prompt you to provide this information either directly, or through a website.

2) **VISHING** is an abbreviation for voice phishing. Perpetrators pose as tech support and request remote access to your computer.

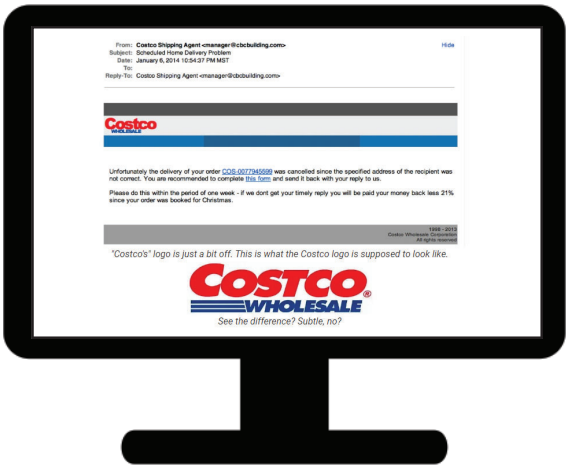
3) **CREDENTIAL REUSE** occurs where an attempt is made to gain access to multiple different accounts using compromised credentials. Cybercriminals may get access to this data either from unsecured database on the web or purchase stolen credentials from a third party. Once they acquire this data, cybercriminals may use those credentials to attempt to login to other accounts. This is why it is important to have different passwords, on each system you login to.

   The use of a second factor for authentication provides greater protection against this attack as logins become time-sensitive and made possible only by the user. Client Access now provides this feature for you to use

4) **MALICIOUS SOFTWARE** is code inserted into a computer system to compromise that system's security. The entry point to a system could be a click on a website, the opening of an email attachment, or installation of pirated or unknown software.

Phishing Example

Below is a classic example of a phishing email, which on the surface seems rather legitimate. However, don't be fooled. Did you notice the Costco logo was just a bit off? Don't just check the name of the person sending you the email. Check their email address by hovering your mouse over the 'from,' address to make sure no alternations (like additional numbers or letters) have been made. Legitimate companies have domain emails. This email is coming from an address ending in @cbcbuilding.com. This should raise some red flags.



Protecting yourself against these kinds of threats requires ongoing effort and diligence. Here are our top tips to safeguard and reduce the risk of your information becoming compromised.

Top Tips – Safeguarding Your Information

Utilize Our Secure Message Center

- Our secure and encrypted messaging system is available through your desktop and mobile Client Access Account (step by step guide below).
- This is the best way to communicate sensitive and confidential information with our team because it protects your data if your email account is compromised
- Sensitive data includes items like: account numbers, social security numbers, and dates of birth.

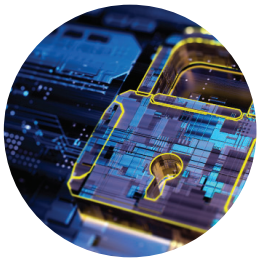
Passwords & Security

- Utilize robust passwords, updating them regularly.
- Keep software current and employ anti-malware protection.
- Exercise caution and avoid clicking on suspicious links or pop-ups.

Fraud & Cyber Attacks

- Stay informed about cybersecurity developments, especially if organizations you engage with are targeted.
- Exercise caution with unknown caller IDs, websites, and text messages, as they might be phishing attempts.
- Verify URLs to ensure legitimacy, as scammers often mimic authentic organization websites.
- Refrain from sending money through cryptocurrency, gift cards, or money transfers, as legitimate organizations won't demand payment through these channels.
- Never share personal financial information in response to unsolicited calls, emails, or texts.

QR Codes



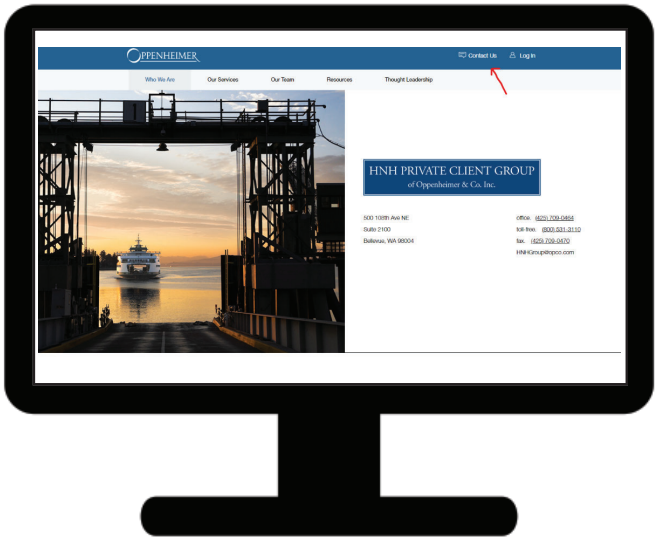
- Be vigilant against malicious QR codes used by scammers for phishing campaigns.
- Avoid scanning unfamiliar QR codes to prevent redirection to phishing sites.
- QR codes in emails are often malicious, as emails can instead display a simple link.

When suspicious of a phone call

- Refrain from disclosing personal information, as voice recordings can compromise your accounts.
- Hang up and contact the company directly using the official number listed on their website.

Accessing Our Secure Message Center – Desktop Version

Go to https://www.oppenheimer.com/client-login.aspx# to login to our client access. Alternatively, you can find our client access website by visiting our webpage.



1) Login using your username and password. If you have forgotten your password, please click on the link that says "Forgot Password." You can also reach out to our team if you need further assistance.
2) At the top right of your navigation bar, click on the message icon to enter the secure message center (see picture below)
3) Once a separate window has opened, click "Compose." This will allow you to send a direct message to our team.

HNH PRIVATE CLIENT GROUP
of Oppenheimer & Co. Inc.

This material is not a recommendation as defined in Regulation Best Interest adopted by the Securities and Exchange Commission. It is provided to you after you have received Form CRS, Regulation Best Interest disclosure and other materials.

© 2024 Oppenheimer & Co. Inc. Transacts Business on All Principal Exchanges and Member SIPC. 6506700.1