Staying Safe in the Digital World

A Cybersecurity Awareness Guide for C2 Clients

This material is intended for existing C2 clients only and is provided for educational and informational purposes only. Material does not constitute investment, legal, or tax advice.

The Password Problem, and the Fix

WEAK — AVOID THESE

- 123456 / password / qwerty123
- FirstNameYear (Karen1958, Bob1955)
- PetName + Numbers (Fluffy2023)
- Same password everywhere
- Any single dictionary word
- Anything under 10 characters

STRONG PASSWORD RULES

12+ characters minimum

Longer = exponentially harder to crack

Use a passphrase

e.g. 'CoffeeLake$BlueSky#42'

Unique password per account

One breach won't expose everything

Enable 2FA on every account

Covered in full on the next slide

Recommended: iPhone iCloud Keychain or Bitwarden are both FREE and available today.

How to Handle a Suspicious Email in 3 Steps

Never act from the email itself. Always verify independently.

1

STOP

Don't Click Anything

Don't click links. Don't open attachments. Don't reply. Even if the email looks 100% legitimate, if something feels off, trust that instinct.

2

VERIFY

Go Direct to the Source

Open a new browser window. Type the company's address yourself. Check for real alerts from there. Never use any link or button from the email.

3

REPORT

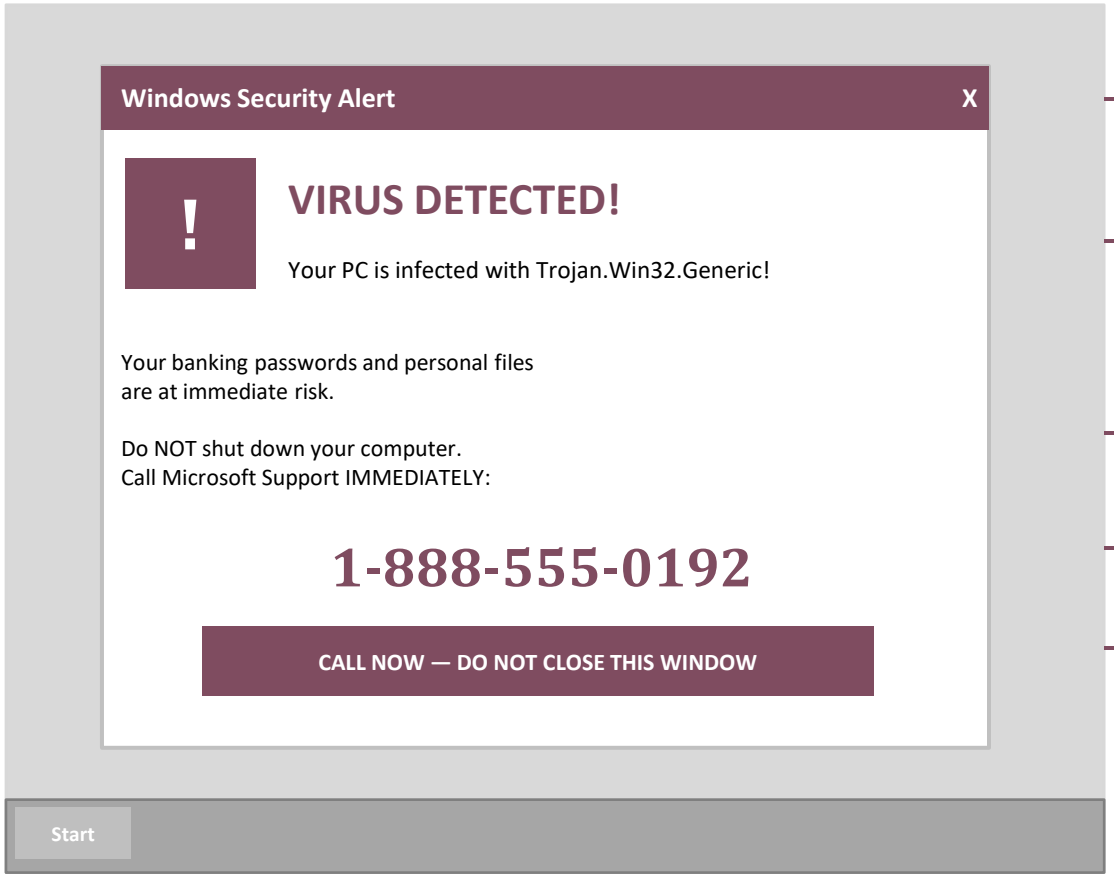
Tell Someone

Forward to reportphishing@apwg.org.
File at ReportFraud.ftc.gov.
Call C2 directly if any financial accounts may be involved.

C2 Private Wealth will NEVER email requesting passwords, account numbers, or wire transfer instructions.

EXAMPLE: The Fake Tech Support Pop-Up

SIMULATED EXAMPLE



1 Microsoft NEVER shows phone numbers in browser alerts

2 Fake virus name — designed to sound technical

3 "Don't restart" prevents you from simply making it stop

4 Not Microsoft's number — may cost $10+/minute

5 Urgency + fear = the formula for every scam

If You've Been Targeted

Do not be embarrassed. Being targeted does not make you foolish.

1

Call Your Bank

Call your bank immediately. Wire transfers can sometimes be recalled within hours. Don’t wait.

2

Report FBI

File a report at **ic3.gov**, the FBI’s official cybercrime portal. It's FREE and only takes 10 minutes.

3

File with the FTC

ReportFraud.ftc.gov, the Federal Trade Commission (FTC) tracks fraud patterns and pursues large operations.

4

Call C2

If any financial accounts are involved, call us immediately so we can coordinate with custodians.

These are professional criminal organizations. What matters now is speed.

How C2 is Working to Help Protect You

We use the following processes to enhance your safety:

- ✓ Trusted contacts on file with Fidelity and C2
- ✓ Mandatory phone verification for key transactions
- ✓ Secure processes for changes to account structure
- ✓ Custodian-enforced signature requirement, 3rd-party withdrawals
- ✓ Alerts and monitoring for unusual trading activity
- ✓ **NEW: C2 Escalation Process if unusual activity or behavior is noticed**
- ✓ **NEW: Two-factor authentication for one-time distributions or withdrawals**

Critical Next Steps for You

- ✓ Ensure you have added a non-spousal trusted contact to your C2 profile at myc2pw.com/trustedcontact
- ✓ Opt into two-factor authentication for added security.

SCAN TO ADD TRUSTED CONTACT

Reflects current firm and custodian practices, which are subject to change. No security measure can guarantee complete protection against fraud.
Clients are encouraged to review account statements regularly and report any suspicious activity immediately.

Your Personal Cybersecurity Checklist

One-time investment. About 30 minutes at home. Significant, long-term protection.

PASSWORDS

- [ ] Use a password manager (iPhone Keychain, Bitwarden, 1Password)
- [ ] Unique password for every important account — never reuse

VIRUS PROTECTION

- [ ] Windows Defender is sufficient for most home use — leave it on
- [ ] Run only one antivirus program; never stack two together

EMAIL & TEXTS

- [ ] Never click links from unknown or unexpected senders
- [ ] Verify the sender domain before opening any attachment

TWO-FACTOR AUTHENTICATION

- [ ] Enable 2FA on email, bank, and investment accounts
- [ ] Use an authenticator app rather than SMS codes where offered

ACCOUNT HYGIENE

- [ ] Check haveibeenpwned.com for your email address
- [ ] Review which third-party apps are connected to your accounts

PHONE

- [ ] Add a carrier SIM transfer PIN; register at donotcall.gov
- [ ] Hang up on anyone demanding gift cards or wire transfers

This webinar has been prepared by C2 Private Wealth for educational and informational purposes only. The content presented does not constitute investment, legal, tax, or cybersecurity advice, and should not be relied upon as such. Individual circumstances vary; clients are encouraged to consult qualified professionals regarding their specific situation.

Statistical data referenced throughout this presentation has been sourced from third-party organizations including the FBI Internet Crime Complaint Center (IC3), the Federal Trade Commission (FTC), CrowdStrike, and Microsoft. C2 Private Wealth has not independently verified the accuracy of this data, and figures are subject to revision.

The cybersecurity practices and recommendations discussed are intended as general guidance only. C2 Private Wealth does not guarantee that implementation of these practices will prevent fraud, data loss, or unauthorized account access.
C2 Private Wealth maintains written policies and procedures designed to protect client information consistent with applicable regulatory requirements, including Regulation S-P. Clients with questions about their account security or C2 Private Wealth's information security practices are encouraged to contact us directly.

C2 Private Wealth is a registered investment adviser with the U.S. Securities and Exchange Commission. Registration does not imply a certain level of skill or training.