7 TIPS FOR PROTECTING CLIENT INFORMATION

YOU CAN NEVER BE TOO SAFE WITH YOUR CLIENTS' DATA.

TO SECURE THEIR DATA AND YOUR REPUTATION, CONSIDER DEVELOPING A MULTI-LAYERED SECURITY APPROACH WITH THESE STEPS.

1. COMPLETE SECURITY TRAINING

EACH STAFF MEMBER IN YOUR FIRM SHOULD GO THROUGH CYBERSECURITY TRAINING TO UNDERSTAND SECURITY PROCEDURES AND HOW YOU CAN CORRECTLY USE TECHNOLOGY TO PROTECT CLIENT DATA.

2. KEEP YOUR SOFTWARE & BROWSER UPDATED

ALL SOFTWARE, INCLUDING YOUR WEB BROWSER, SHOULD BE UP TO DATE TO COMBAT CYBERCRIMINALS.

PRO TIP: CONSIDER RUNNING A BROWSER EXTENSION CALLED HTTPS EVERYWHERE TO VERIFY ALL WEBSITES YOU VISIT ARE SECURE.

3. RUN A ROBUST ANTI-VIRUS

ALWAYS HAVE ANTI-VIRUS SOFTWARE RUNNING IN YOUR COMPUTER'S BACKGROUND. PRICELESS IN TODAY'S AGE, ANTI-VIRUS PROGRAMS DETECT PROBLEMATIC MALWARE, WEBSITES, AND EMAILS.

4. DON'T FALL FOR PHISHING

FRAUDULENT PHISHING ATTEMPTS SEEK TO GET SENSITIVE INFORMATION FROM YOU LIKE PASSWORDS, CREDIT CARD INFORMATION, AND MORE. PHISHING IS THE PRIMARY CAUSE OF DATA BREACHES, SO EDUCATE YOURSELF ON THE WARNING SIGNS FOR THESE TYPES OF ATTEMPTS.

5. USE A FIREWALL

FIREWALLS ARE A NETWORK SECURITY TOOL THAT PROTECTS AGAINST A VARIETY OF ONLINE THREATS. CONSIDER GETTING A UNIFIED THREAT MANAGEMENT (UTM) APPLIANCE TO PROTECT AGAINST ONLINE INTRUSIONS.

6. IMPLEMENT TWO-FACTOR AUTHENTICATION

WHEN AVAILABLE, EMPLOY TWO-FACTOR AUTHENTICATION (2FA) FOR YOUR ONLINE ACCOUNTS. 2FA SENDS A CODE TO YOUR MOBILE PHONE WHEN LOGGING IN TO VERIFY THAT IT'S REALLY YOU. IT ADDS A QUICK AND EASY LAYER OF SECURITY.

7. SECURE YOUR WIRELESS NETWORK

WI-FI EXTENDS OUTSIDE YOUR OFFICE WALLS. AND IF YOUR WIRELESS NETWORK ISN'T SECURED, YOU'RE MAKING YOURSELF AN EASY TARGET FOR A CYBERCRIMINAL. THINK ABOUT ADDING THE WI-FI PROTECTED ACCESS 2 (WPA2) SECURITY METHOD, TOO.

** For Internal and Advisor Use Only - Not for Customer Use*

FINANCIAL INDEPENDENCE GROUP®