Total Technology Solutions

November 2016 Edition

Newsletter

Dangers of Public WiFi

We've all been there, suddenly while out running errands, you remember that you have something urgent to do and you simply forgot. "Ooh, I have my phone," you say realizing that you can pay your bill right here and now or buy that toy for your kid's birthday so that it arrives on time...NOW. Everything is accessible here and now! You think, "Let me connect to the WiFi. I can't exceed all of my data this month and get another $500 phone bill." But did you know that using Public WiFi (the Guest WiFi at the doctor's office or the airport WiFi) can be dangerous.

Tip 1: Only Send Information to Encrypted Sites

Websites that are encrypted take any information you submit over the Internet and scramble that information into a code that makes it inaccessible to others. You can check if a website is encrypted by looking at the beginning of the web address for ***HTTPS***. And don't just stop there. Be sure to check every page that you visit on that website for it to begin with ***HTTPS*** as some websites don't use encryption across the entire website. If any part of your website session is not encrypted, your information is vulnerable.

Tip 2: Be Wary Using Mobile Apps

It is more difficult to tell whether or not a mobile app is encrypted because you cannot see the visible ***HTTPS*** indicator. So it is important to use caution when entering any personal or financial information on a mobile app when the WiFi is not secure. In fact, research suggests that many mobile apps are not properly encrypted so it is important to protect yourself and your data. As a precaution, if you are accessing a public WiFi, you should check the mobile website (instead of the app) for the ***HTTPS*** before performing a potentially unsafe transaction.

Tip 3: Don't Assume a Hot Spot is Secure

If your phone or device detects a WiFi hotspot and a password is not required, it is more than likely not secure. There are free online hacking tools that allows hackers to take over an online session and log in as you, potentially accessing your personal information, contacts, photos, and even login credentials. As recommended with mobile apps, only use a Hot Spot WiFi connection for personal information transactions on websites that you are sure are fully encrypted.

Tip 4: Always Log Out and Vary Login Passwords

To keep yourself protected in case of a potential hack, it is important to log out of your accounts at all times. If you don't log out, you're leaving a window of opportunity open for unwanted access. Also, as an extra precaution, it is recommended to vary your passwords across accounts. This makes it more difficult for a hacker to access other accounts if your information is, in fact, compromised.

Quiz: Internet Security

Take this short quiz to see if your business is at risk (answers at the bottom)

1. What should you do to close an unwanted pop-up window?
   a. Click **OK** or **Close**.
   b. Click the **X** on the window.
   c. Press Alt + F4.

2. True or False. If you use a public WiFi network that assigns you a password, it is okay to send confidential data out.

3. True or False. If you are using Windows XP or Microsoft Office 2003, you are receiving periodic security updates.

4. True or False. If your data is breached, you are required to file a report and alert all potential customers.

5. Of people who were victim of online fraud, the average financial loss was between:
   a. $0-$999
   b. $1,000-$4,999
   c.. $5,000-$9,999
   d. $10,000+

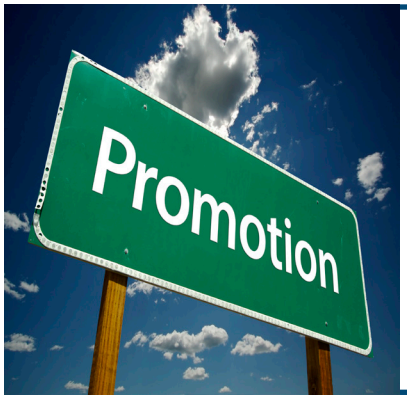
6. True or False. If you have installed all of the latest the security updates required by your system administrator, you still need to be cautious when clicking links and opening attachments.

Answer Key: 1.c; 2. F; 3. F; 4. T; 5.b; 6. T

Are you interested in attending one of Total's Lunch & Learns? Topics include Cyber Security, Business Continuity, and more. Call us today at 888-777-8093 to reserve a spot for our next Lunch & Learn.

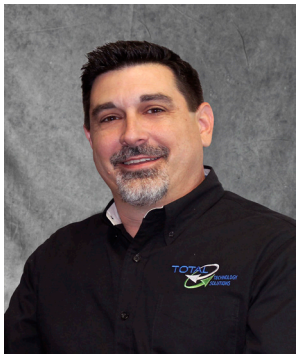
TOTAL TECHNOLOGY SOLUTIONS

HEADQUARTERS: 1895 Walt Whitman Road • Melville, NY 11747 USA
631-777-7477 • 888-777-8093
www.total.us.com



Total is extremely excited to share the promotion of its 16-year veteran, Chris Repetti, to Chief Technology Officer (CTO). Prior to his new role, Chris was a Senior Network Engineer who has demonstrated exceptional leadership, dedication and intimate knowledge of the industry, clients, operations, products and engineering.

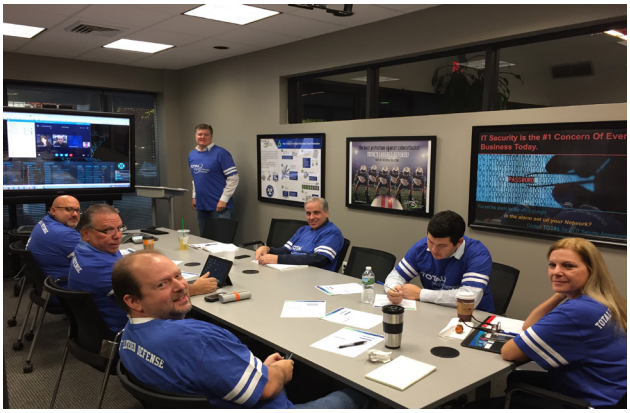
Vincent Tedesco, President & CEO of Total believes Chris's enriched vision and expertise will help Total build an even closer linkage to client support both today and in the future. "I view product management and engineering as a continuum in the delivery of client solutions, and Chris as the perfect leader to align our priorities as our new CTO," says Tedesco.



We Practice What We Preach

Total wrapped up National Cyber Secuirty Awareness Month (NCSAM) during the last week in October with a staff training focusing on Total's Layered Defense. As the name of the offering suggests, the solution is layered, meaning that we utilize multiple security solutions, policies and procedures to tailor security programs that ensure safety and business continuity.

This training was conducted by Total's Security as a Service Committee who is in charge of continuously analyzing new security services, as well as investigating new vulnerabilities recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In an attempt to stay ahead of the cyber crime curve, this training focused on educating Total's staff on new technologies that may be able to further help mitigate potential cyber attacks for clients. Because of the sophistication of hacking methods across the globe, Total continuously reviews the offering and makes necessary improvements to it.



As a follow-up to this training, Total's staff is also attending an Employee Awareness Cyber Security Training this month. Awareness Training is one of the many "layers" of the cyber security solution and is probably one of the most important defenses for protection.

Total was recently a sponsor of Casino Night for the Variety Child Learning Center (VCLC). The event took place on October 19, 2016 at the Chateau Briand in Carle Place, NY honoring the center's 50th anniversary.

VCLC is a not-for-profit center providing special education programs for children who reside in Nassau, Suffolk and New York City, with developmental and learning disabilities, including autism, along with programs and support services for families.

As a long-time supporter of the United Hospital Fund (UHF), Total continues to support the organization's annual Campaign for a Healthier New York.

United Hospital Fund

As an independent, non-profit organization, UHF works to build a more effective health care system for every New Yorker by analyzing public policy to inform decision-makers, finding common ground among diverse stakeholders, and developing and supporting innovative programs that improve the quality, accessibility, affordability, and experience of patient care.

TOTAL TECHNOLOGY SOLUTIONS

HEADQUARTERS: 1895 Walt Whitman Road • Melville, NY 11747 USA
631-777-7477 • 888-777-8093
www.total.us.com