classcomputing

CLASS NOTES FD October 2016

*"Insider Tips To make Your Fire District Run Faster, Easier And Increase ROI"*

## What's New

**Please submit your questions now:**

**ask@classcomputing.com**

**"How can I do this task with this software or hardware?"**

**Or submit technical questions you need answered. It will be anonymous, we will post the question and publish the answers as they come in. Remember, we are "your in-house IT department".**

**UPDATE: A few people took advantage Of this offer. We are astonished more people did not send in questions. Please feel free to get some free help. If you submitted a question and did not get an answer, there is a chance we did not get the email. Please CC the following: sales@classcomputing.com**

**You are busy and don't have time to learn the nuances of your tech, gadgets and software.**

**That is the beauty of this forum. All the answers are here, we just need to Utilize the hundreds of years of experience of the readership.**

## October 2016

*A message from the owners...*

"As a Fire District, you do not have time to manage the operational AND Technical issues. That is where we have your back ! Call us and put an end to your IT problems finally & forever !"

Dale & Mark,
Class Computing

# The One Attack No Tech Can Stop

You can defend your data with all the latest and best technology. But if just one team member gets tricked into giving away the keys to the castle, it's game over. Hackers know this. And that's why so many use social engineering to break in.

And it's not just the big companies you hear about on the news. On February 3, 2016 a suspect posing as the CEO of Magnolia Health Corp. obtained a spreadsheet with sensitive data about their employees. On February 23, someone posing as an employee of Central Concrete Supply Company obtained confidential W2 records and disappeared with them.

In a 2011 survey, Check Point Software Technologies found that nearly half of the companies surveyed reported one or more social engineering attacks resulting in losses ranging anywhere from $25,000 to $100,000 per occurrence.

Unfortunately, there just aren't any whiz-bang tricks or tools that will automatically prevent a clever "social engineer" (SE) from breaking in. The keys to protection are awareness and vigilance. To help you know what to watch for, here are five common ploys - and how to deflect them:

Familiarity - In this type of scheme, the hacker becomes familiar to an employee. Social networking sites can reveal an employee's schedule and favorite hangouts. The hacker might then frequent the same bar or restaurant. After a drink or two, some key fact may slip out... The best way to bust this ploy is to be careful to not get lulled into a false sense of security around people you haven't thoroughly vetted.

The Consultant - A social engineer poses as a consultant for

*continued on page 2*

hire. Once they get the gig they can scoop up all the info they need from you and your team because of their seeming authority. Watch for this especially with IT consultants. Do NOT trust blindly. Vet every consultant, and never give all the keys to the kingdom. Just because someone has the skills to fix your server or network doesn't mean they won't steal your data. Vet thoroughly, and, as Ronald Reagan said, 'trust but verify'.

> "When you see THIS exploit unfolding…. **call security**."

Piggybacking - The SE waits by a secured door for someone to use their passcode and enters right behind them. Or the SE struggles with a heavy box and asks a legit employee to hold the door open for them. Being kind and helpful, the employee helps the SE right into the building… free to do as they please. To foil this one, never forget the dangers of allowing a stranger in without proper clearance.

The Interview - Key information often escapes during interviews. A smart social engineer will gain an interview and deftly pick up all the information they need to hack into your network. Make sure any data provided during an interview offers nothing in the way of secrets. Keep the conversation light, or even superficial to avoid leaking critical data.

Angry Man - You may have seen this on TV… Somebody has an angry tone on the phone, or is grumbling to themselves as if they've just had an argument. We all tend to avoid people like that. Enough people avoid them and the way is cleared into the heart of the company - and your data. Don't go along with it. When you see this exploit unfolding, call security.

The key to preventing social engineering attacks is a well-trained workforce. You and your people may be your company's greatest asset. Yet without regular, proper training, human beings can be the weakest link in your company's data defenses.

Here's how to protect your network from a costly cyber attack as a fellow business owner in the **Chicago** area, I'd like you to take advantage of my extensive research and experience in protecting data networks for small and medium companies. My business owner's guide:

**The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind**

steps you through 10 ways to protect your company from the coming deluge of cyber attacks we can expect over the next several years and beyond.

You have worked way to hard to get where you are today to risk it all to cyber-villains.

**CALL TODAY (312) 262-3930**
or email me to get yours **FREE**
**sales@classcomputing.com.**
We still have a few of the hard copy versions I'd like to send you, so call or email me now while they're still available. I look forward to sending you this valuable guide right away.

## Help Us Out And We'll Give You A Brand-New *Amazon Fire 7* For Your Trouble

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of **October 2016**.

Simply refer any Company or Fire District with 10 or more computers to our office to receive a FREE Computer Network Assessment (a $397 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free ***Amazon Fire 7*** as a Thank You or Donate $100 to your favorite charity! Simply **Call Us** at **(312) 262-3930** or drop us an e-mail at with your referral's name and contact information today! **sales@classcomputing.com**

*"You are only as good as your Tools."*

**Panasonic Toughbook 20**
The fully rugged, detachable laptop combines the features of a laptop and a tablet, and is purpose-built for challenging environments[1]
( 1. Article Source, Date )

**The new Panasonic Toughbook 20 is a fully rugged, detachable laptop that combines the features of a laptop and tablet.**

The Toughbook 20 is purpose-built for challenging environments, including health care, public safety and defense.

It offers six usage modes. Besides being used as a traditional laptop, the tablet can be detached and used by itself or flipped 180 degrees to show content in presentation mode. Using the built-in handle, the device can operate in carry mode or hanging on a wall, while vehicle mode provides full functionality and operation when on the move.

The device features a 6th Generation Intel CoreTM vProTM processor technology, 128GB SSD, 8GB RAM and choice of Windows 10 Pro or Windows 7 Professional.

The Toughbook 20 is designed to meet MIL-STD-461F for electromagnetic interference and MIL-STD-810G for drop, shock, vibration, explosive atmosphere, temperature, humidity, rain and sand, as well as waterproof and dustproof ingress (IP65).

The device features a magnesium alloy case, fanless design, locking port covers, raised bezel, Solid State Drive (SSD) heater and a built-in handle, which also serves as a kickstand for desktop stability and enables use while hung.

Panasonic Toughbook 20 aims to enable productivity inside and outdoors, featuring a 10.1" sunlight-viewable 800 nit IPS display with gloved multi touch capabilities, a waterproof stylus pen and a backlit keyboard that is 16 percent larger than the Toughbook 19. It also features a 2MP webcam and an optional 8MP rear camera. Other optional features include a bridge battery for continuous operation and a second battery to double battery life.

**Call Class Computing today for the latest pricing on this amazing hybrid laptop by Panasonic (312) 262-3930.**

# NEW MAC MALWARE COULD SECRETLY RECORD YOUR WEBCAM DURING VIDEO CHATS

By Mihăiță Bamburic Betanews.com

FBI director James Comey made the news last month when he admitted that he tapes over his laptop's webcam to avoid being spied upon. Mark Zuckerberg does it too. As Comey puts it, blocking the webcam is a "sensible" thing to do -- and if you too care about your privacy you should follow suit. But, there is a problem.

When you remove the tape to chat with someone you are left vulnerable. And, as a security researcher will demonstrate today at the VB2016 conference, a hacker could use that opportunity to record Mac users' activities "in an essentially undetectable manner".

Patrick Wardle, the director of Research at Synack and a former NASA and NSA employee, has devised an "attack" that enables malware to monitor a Mac and only record the video sessions when the webcam is in use. It is clever, because that is when you expect the little green indicator next to the webcam to be lit up. Wardle says that the webcam indicator light on Macs is hardware-based, suggesting that it may not be possible (or likely) to power up the webcam and hide the fact that it is on from the user -- like it can be done on other devices.

"As there are no visible indications of this malicious activity (as the LED light is already on), the malware can record both audio and video without fear of detection", Wardle explains. Basically, it is signaling the fact that it is making use of the webcam, but because a legitimate app, like FaceTime or Skype, is also using it the user has no reason to suspect that they are being secretly recorded by a third-party.

The good news is that Wardle says there are ways to detect when the webcam is used in such a way by malware, and that there will be a free tool for macOS and OS X users that features a detection mechanism and offers alerts when this attack is being carried out.

There is no word on whether Apple can block this piggyback method in a future operating system update, but it should be possible given what Wardle claims. Also, seeing as this is a new attack, there is a fair chance it has not been exploited yet by another party.

**CLASS COMPUTING is very passionate about Hardware and Gadgets! This includes Cellular Products and Remote Computing. Remember, Hardware is part of the Network...we manage your entire companies IT, so shouldn't we consult you on the hardware too?**

**CALL US AT (312) 262-3930.**

NATIONAL FALLEN FIREFIGHTERS FOUNDATION

**35th Annual National Fallen Firefighters Memorial Weekend October 8-9 2016**

**http://www.firehero.org/events/memorial-weekend/attending-memorial-weekend/**

NATIONAL FALLEN FIREFIGHTERS MEMORIAL 2015 WEEKEND

**https://www.firehero.org/donate/**

## Hot Sellers Last 60 Days

**Toughpad FZ-G1**

**Toughbook 54**

## Gaining Interest Last 60 Days

**Getac F110**

**Getac RX10**

## Who Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month's Trivia Challenge Quiz is…

**Joe Ostrander of Tri-State FPD**; he was able to answer the question from September:

**If 2 of every 5 fires starts in the kitchen and 60% of all kitchen fires is started by the range, what percentage of ALL fires are caused by the range?**

**40% (B) 34% (C) 24% (D) 60%**

**The correct answer was (C) 24%**

Now, here's this month's trivia question specifically for Fire & Rescue.

**The winner will receive a $25 VISA® gift Card.**

**With respect to fire...when you see the words Fuel, Heat, Fire, Oxygen, 21%; What is the logical shape that corresponds?**

(A) Circle (B) Square (C) Triangle (D) Star

**E-mail Us Right Now With Your Answer.**

(We put all correct answers in a hat, and choose 1 to get the Gift Card.)

**sales@classcomputing.com**

## GETAC®

**Absolute DDS**

This optional protective measure disables your F110 if it detects an unauthorized or compromised entry.

**Trusted Platform Module 2.0**

The F110 features TPM 2.0 – a powerful anti-tampering device that checks for any signs of intrusion during system boot-up.

**Fingerprint Scanner**

Verify your ID with ease and accuracy by simply swiping your finger.

**NFC/RFID Reader**

Authenticate your credentials via Near Field or Radio Frequency transmission.

**Smart Card Reader**

The F110 supports Smart Cards for secure identity verification.

**Windows 10 Multi-Factor Authentication**

The F110's hardware fully supports Microsoft's latest authentication tools, including Windows Hello, Microsoft Passport and Credential Guard.