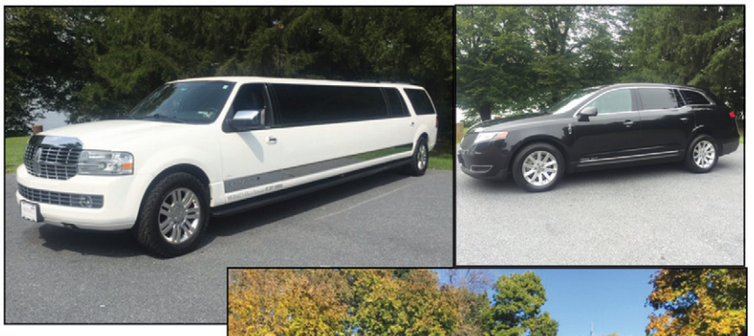
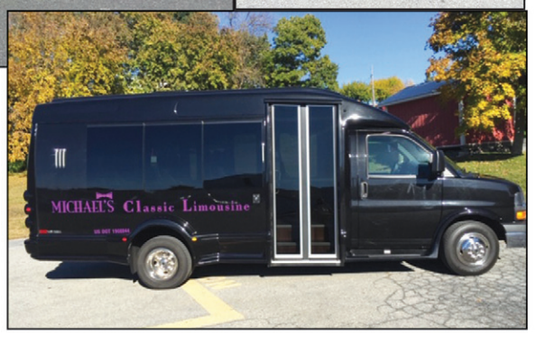
www.michaelsclassiclimo.com

610.929.4919





Arrive in Style!

Well-maintained, chauffeur-driven luxury vehicles for any occasion.

41 North Centre Avenue
PO Box 206 Route 61,
Leesport, PA 19533

PUC-A-6410449

RECOGNIZING A CYBERATTACK

SAVE YOUR DATA BY LOOKING FOR THESE SIGNS

TECH TIPS

By Kelly McNeil, TechBldrs, Inc.

It may not have hit the headlines like the Coronavirus or election season, but the United Nations recently suffered a major security breach. A vulnerability in their system — caused by a failure to patch a known problem! — was exploited by hackers to hit a variety of targets world-wide. What does the fact that the UN is lagging behind on necessary cybersecurity precautions mean for the rest of us?

Software manufacturers spend millions of dollars a year on patching security flaws and releasing those fixes to their customers. The hole in the UN's security should have been patched by their IT staff within a month of the release of the patch, but it wasn't. Instead, the UN was left wide open to the attack, which was likely orchestrated by an organized group of hackers, and could likely have been helped along by someone within the UN clicking on something they shouldn't have. The extent of the breach remains unknown, but reports suggest that the thieves made off with a catastrophic 400GB of data to now do with what they please.

This is a situation caused by negligent IT support — but could an employee have helped stopped the breach in its tracks by recognizing a few key signs?

Here's how you recognize a cyberattack in progress, and here's what you can do to try to limit the damage it does.

1. A strange email

Sometimes an email will just look "wrong" to you — whether it comes from an unknown sender, or asks you to accept a payment you never requested, or any other suspicious activity, trust your gut! If it was supposedly sent by someone you know, give them a call or talk to them in person to confirm. Don't click on any links, open any attachments, or reply to the email, just delete it before a hacker uses it to cause damage.

2. A suspicious error message

Sometimes it's the entire screen, sometimes it's just a window, but an error message you don't recognize and doesn't look "official" is never good. When it doubt, don't click on *anything*, just crash your system: hold down the power button of your computer until it shuts off, or pull your computer's plug out of the wall. Crashing your system will power down your computer and stop an attack in its tracks.

3. Calls or emails from a service provider

Always verify calls or emails from Microsoft, your bank, or any other service provider you use. Hackers who already have some of your information may try to swindle you into giving them more than what they have by impersonating a trusted company, like Netflix, American Express, or Facebook.

(Continued on page 52)

Working hard for local businesses, local families... local everything.

WSFSBANK.COM / 1.888.WSFSBANK

WSFS bank
We Stand For Service®

EQUAL HOUSING LENDER Member FDIC

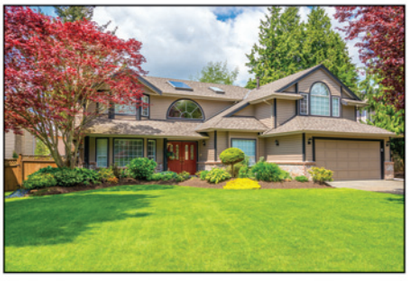
Affordable Luxury
Financing for everyone with rates a low as 2.49%
Guaranteed Credit Approval • All Income Types Accepted

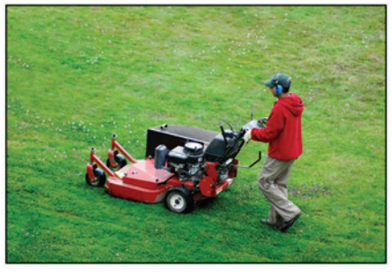
highstreet AUTO CONNECTION

1415 W. High Street, Pottstown, PA 19464
484.624.3120
www.HighStreetAutos.com
Make your next move your best move right in town at High Street Auto Connection.

SOTTOSANTI
LAWN • CARE
Serving Berks County Since 1978

- Landscape design and installation
- Hardscaping
- Patios
- Walkways
- Retaining walls
- Sod and seed lawn installation
- Excavation
- Snow removal
- Lawn mowing and maintenance
- Spring / fall cleanup
- Edging and mulching
- Shrub trimming and removal
- Fertilization and aeration
- Tree and shrub installation and maintenance





We Can Help You Create the Outdoor Living Space of Your Dream!

Residential
Commercial
Free Estimates
Fully Insured

We're big enough to get your job done and small enough to know your name!

610.670.7639 • 610.370.1507
www.sottosantilawncare.net

VSPOT
WOMEN'S INTIMATE HEALTH SPA

V-Tightening
V-Lightening
V-Steam
O-SHOT®
V-Plump
BTL EMsella™ aka "Kegel Throne"
BTL EMsculpt™
Vampire Breast Lift®
24k Gold Wax & LED Vajacial
FemiLift™

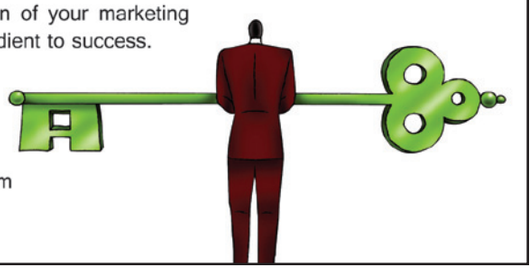
At VSPOT, our mission is to educate and empower women through non-invasive intimate health solutions. Women face many transitions throughout the natural aging process, from menstruation to childbirth to menopause.
These changes greatly impact daily life!

Our treatments allow women to care for all facets of their well-being - *including their intimate health.*

1920 Chestnut St., 2nd Fl | Philadelphia, PA 19103
267-534-3355 | vspotmedispa.com

JWM Business Services
we put your marketing in motion
JWM Direct
Way Cool Email
Kinetic Web Solutions

Proper implementation of your marketing ideas are a key ingredient to success.



www.jwmbusiness.com
610-831-9030

Tech Tips

(Continued from page 50)

If something doesn't seem right, hang up/don't click on anything in the email and contact the company's support service to confirm if the person that contacted you was really working for them or not.

4. You're locked out of your computer, but you don't remember trying to logon

If a hacker has your username and/or password (or any you've used in the past), they'll often try to brute force their way into your computer to gain access to your information. In other words, they'll keep trying over and over to guess your username and password combination in hopes that they'll eventually guess correctly. Your computer may lock them out after a certain number of tries, so if you find yourself on the receiving end of a "too many login attempts" error message, hackers may be trying to gain access.

5. Unknown software appears and/or begins installing without your permission

Hackers will often install spyware or other malicious software on your computer once they've gained access. Or it may download automatically after you've clicked something you weren't supposed to! If you don't recognize a program that's running on your computer, or something you haven't authorized begins to install, immediately power down your computer.

6. Your email suddenly stops working

If it's been a suspiciously long time since you've gotten an email and emails you've sent are appearing as unsent, it could be a sign that someone else has access to your account. If you think this might be the case, it's time for a cybersecurity professional to help you — they can determine if it's any cause for concern, or if your email's just on the fritz.

7. Your mouse/cursor moves intelligently on your screen on its own

While we've all seen our mouse move when we bang our knee on our desk, one of the surefire ways to tell if someone's actively accessing your computer is if your mouse is moving like it suddenly grew a brain of its own. Clicking on folders, accessing files, or opening your system settings are all signs that someone else is using your computer. If you ever see this happening, immediately power down your computer and call in professional help.

While remaining vigilant and educated about cybersecurity is your best line of defense against hackers and other criminals, we always recommend calling us if you think you've been on the receiving end of these (or any!) signs of cyberattack. If the UN can get hacked, so can you, and so can your business.

If you want to schedule a cybersecurity education session for your company, want a free Dark Web scan of your company's email addresses, or have any questions about this article or other cybersecurity concerns, you can call TechBldrs at 610.937.0900 or email us at info@techbldrs.com and visit our blog at www.TechBldrs.com.

ROUTE 422 BusinessAdvisor
Promote your business in the Route 422 Business Advisor! Call (610) 323-6253