# The TMC ADVISOR

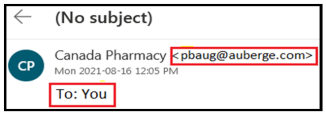
*The Advisor is a periodical published by TMC containing articles of interest to Canadian Business Professionals* *Nov 2021, Vol 8 # 5*


## Identifying Email Phishing *By Ellen Koskinen-Dodgson*

Pretty well everything you don't want to happen can happen through phishing attacks — a user is tricked into clicking on a link, opening an attachment, or disclosing information. Everyone knows that we shouldn't fall for a phishing attack, but what exactly does that mean? We can't delete every email that might possibly be dangerous. Here are some simple ways to check out a questionable email message.

***An Easy Example***

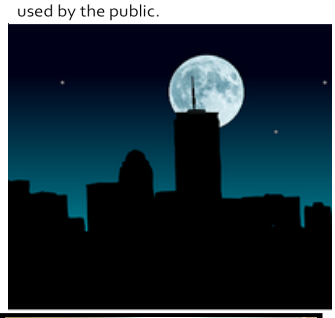
Here's a malicious email with obvious red flags.




The first red flag is that 'Canada Pharmacy' is not one that is generally used by the public.

## Telecom Service During a Disaster *By Peter Aggus*

Old school analogue telephone service was powered from the telco office and was almost bulletproof. When all else failed, you could go to the designated power fail phone and dial the world. These days, telephony is part of data networking so often will not work during power outages. Worse, unknown damage some distance away from you can affect your service thanks to the way providers have designed their networks.



## How Do You Rate?

Our IT Assessment Team can identify and explain how you compare to best practices on:

- Reliability
- Staffing Levels
- Costs
- Customer Service

For a free copy of "What to Assess and Why," email: assessment@tmcconsulting.ca.

## Needed: Flashlights *By Guy Robertson*

What happens in a business office at the beginning of a power outage? Overhead lights snap off. Dim emergency lights turn on in the hallways as you sit in the near dark, trying to decide if the lights will come back on quickly. Flashlights (real ones) are very useful.

## 9 Future Work Trends Post-COVID-19 *By Maria Colasurdo*

A recent Gartner survey has identified some lasting changes resulting from the COVID-19 pandemic disruption, "large-scale shifts that are changing how people work and how business gets done". These trends will form the scorecard on how you are judged against your peers and will likely mean that you need to revisit both your Strategic Plan and your Business Continuity Plan.


ISSN 2369-663X21

# Identifying Email Phishing *By Ellen Koskinen-Dodgson*

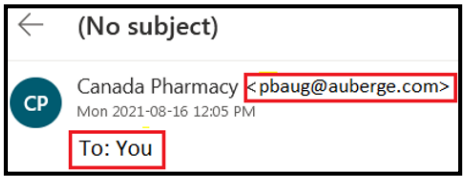
Pretty well everything you don't want to happen can happen through phishing attacks - a user is tricked into clicking on a link, opening an attachment, or disclosing information. Everyone knows that we shouldn't fall for a phishing attack, but what exactly does that mean? We can't delete every email that might possibly be dangerous. Here are some simple ways to check out a questionable email message.

## Phishing is Easy

Phishing is one of the most common types of cyber-attacks – and the most successful. That's because it's so easy to perform. It tries to steal sensitive information such as credit card numbers or usernames and passwords to gain access to your systems. It works because of our curiosity and our willingness to be helpful. The bad guys find your address from the Internet through hacked websites, and from publicly disclosed accounts on public forums.

## An Easy Example

Here's a malicious email with obvious red flags.




The first red flag is that 'Canada Pharmacy' is not one that is generally used by the public.

We use Shoppers Drug Mart, London Drugs, or our regular local pharmacy.

Poorly written messages are also red flags. There is no subject in the Subject Line and the sender's email address does not seem to match very well with the display name of Canada Pharmacy. Also note how the To: field is addressed to 'You'. Reputable companies do not send out emails that look like this.

In this example there are too many red flags to even waste our time trying to check it out. This is a good example of the "just delete the message" approach to suspicious communications.

## A Tough Example


A common spoofed email that's difficult to detect looks like it is from your CEO or a senior executive. It requests a money transfer or an account reset, often from their cellphone and often with an urgent tone.

As frauds are difficult to detect, these type of requests must be confirmed via a voice call or escalated up to senior management for confirmation.

## Red Flags

Be suspicious when you receive an email that seems to respond to a question you didn't ask, or an action you didn't take. Beware if you're asked to click on a link or provide confidential information. If there's anything "off" like poor formatting, grammar, spelling or graphics, just delete it.

## When in Doubt

When in doubt, but you think that the email might be legit, do some basic investigation. Look for red flags, hover over a link to see if the link text matches the visible words, check the message file properties to see the originating email address and the reply to address....

If the message looks important, especially if it deals with banking or other sensitive information, contact the sender using contact information from another source. Never use contact information provided within the suspicious email.

If you're not sure about the source of the message, and it doesn't seem important, just delete it.

If you'd like to comment on this article or explore these ideas further, contact me at ellen@tmcconsulting.ca.

This article is reproduced from the November 2021 edition of *The TMC Advisor*



*Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.*

# Telecom Service During a Disaster *By Peter Aggus*

Old school analogue telephone service was powered from the telco office and was almost bulletproof. When all else failed, you could go to the designated power fail phone and dial the world. These days, telephony is part of data networking so often will not work during power outages. Worse, unknown damage some distance away from you can affect your service thanks to the way providers have designed their networks.

## Where Is the Power?

New school telephony has largely been subsumed into IT and is locally powered. You may have UPS units at your site to allow files to be saved and systems to shut down properly. You may have chosen a more productive option—a generator—and feel that you'll be fine if you lose utility power. This is where the surprises begin.

You need to understand how you're connected to your service provider and whether there is reliable power for every step of that route. Current Telco distribution infrastructure is often not designed for power fail operation, so you may well have IT services at your site but no Internet access and no telephony 'dial tone'.

Fibre sounds like a safe bet as it needs no repeater power but street cabinet switches do—meaning that shared fibre feeding smaller customers is still at risk from outages. Bigger customers may also be out of luck in a power outage as there is intermediate equipment that depends on battery backup too.

Telco broadband co-ax systems are much the same—they mostly run off local street power, with batteries for some degree of backup.

Cellphone networks may seem to be reliable but again you're faced with battery support to cover short power breaks. New base stations do not generally have generator backup.

## An Example

A recent storm isolated many of the big box stores in Victoria, even though they actually had power. Phones and internet were down, caused by an up-island cable failure—meaning callers could not reach them and they could not process real-time credit card transactions.

## How To Get Started

1. You need to ask questions. What services will fail if electrical power goes out? You need to talk about network architecture and service level agreements with your network providers. The answers will form part of your corporate risk register and BCP/DRP.
2. You then need to look at the consequences of lost communications and power—and then decide how your business might function under such conditions.
3. Think about how you'll use your Cloud Services if your Internet access fails.
4. Review your business continuity plan and IT disaster recovery plan. A fast and effective way to find serious weaknesses is to conduct a 'tabletop exercise'.
5. Each weakness needs to be added to the risk register and mitigation plans implemented.
6. The worst issues should be mitigated as a top priority.

When we work with clients to facilitate tabletop exercises the results are often surprising and distressing. We review each component of their connectivity and ask: what will happen if there's a power failure?

What begins as a simple question: will phone service work during a power outage can turn into a useful learning exercise and make your operations more bullet-proof.

If you'd like to comment on this article or explore these ideas further, contact me at peter@tmcconsulting.ca.

This article is reproduced from the November 2021 edition of ***The TMC Advisor***



*Peter, as an engineer & technology management consultant, has developed innovative & cost-effective solutions for clients in many industries.*

# Needed: Flashlights *By Guy Robertson*

What happens in a business office at the beginning of a power outage? Overhead lights snap off. Dim emergency lights turn on in the hallways as you sit in the near dark, trying to decide if the lights will come back on quickly. Flashlights (real ones) are very useful.

## Expect Outages

In North America the risk of an outage is higher than that of a fire, bomb threat, or earthquake. Considering the recent warnings of civil authorities about the potential for regional grid failures, we would be wise to prepare for them. Ignoring the risk is not an adequate response.

Outages can be due to different causes. High winds and winter storms damage power lines and poles. Floods and forest fires disrupt power transmission across regions and lead to prolonged outages. Sabotage of power supplies is another possibility. And every week across Canada, a driver loses control of his or her vehicle, rams a power pole, and sinks an entire neighbourhood into temporary darkness.

## The First Minutes

Sound levels drop as heating and air conditioning lose power. Lighting and computer screens flicker, then die. Emergency lighting systems provide low-level lighting in hallways and stairwells.

One hears expressions of dismay as people realize the implications. A courier at the reception desk complains that he can't read the delivery information on the labels of

packages. A call for help issues from the washroom. Employees discover that their cell phone flashlights don't provide an adequate level of illumination.

## The Flashlight

Every business and residence should have a supply of flashlights. These should be stored in conspicuous locations - at the reception desk, in staff rooms, emergency cupboards, in staff washrooms, and if possible—mounted on walls.

Flashlights really come in handy while people wait to hear if they should go home. Once the go-home order is made, flashlights help people collect their possessions and secure the office before leaving.

Every three months, a clerical assistant or custodian should be assigned the task of making sure that all flashlights work. A good supply of spare batteries should also be available.

## Looking Ahead

If predictions of climate change are correct, then we can expect frequent storms and grid failures, and we should prepare for what some emergency planners refer to as the New Dark Ages.

Happily, most outages will be brief, and lead to nothing worse than spoiled food in staff room fridges and temporary closures. Longer outages might result in IT failures, data loss and injuries.

Nevertheless a few simple preparations can prepare you and your office for any sort of outage. Walk around your office and look for flashlights and spare batteries. Would they be easy to find in a power outage?

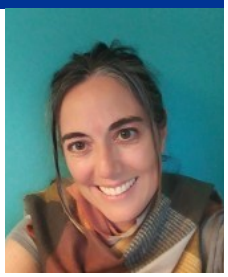
If you'd like to comment on this article or explore these ideas further, contact me at guy@tmcconsulting.ca.

This article is reproduced from the November 2021 edition of ***The TMC Advisor***



*Guy Robertson is a senior planner at TMC and an instructor at the Justice Institute of BC and Langara College. He has written five books and numerous articles on corporate security and disaster planning, and offered workshops and lectures at conferences across North America and in the UK.*

# 9 Future Work Trends Post-COVID-19 *By Maria Colasurdo*



A recent Gartner survey has identified some lasting changes resulting from the COVID-19 pandemic disruption, "large-scale shifts that are changing how people work and how business gets done". These trends will form the scorecard on how you are judged against your peers and will likely mean that you need to revisit both your Strategic Plan and your Business Continuity Plan.

## 1: Remote Work

48% of employees will work remotely at least part of the time after COVID-19 compared to 30% before the pandemic.

## 2: Data Collection

16% of employers are using technologies more frequently to monitor their employees through methods such as virtual clocking in and out, tracking work computer usage, and monitoring employee emails or internal communications/ chat. Some use this monitoring to measure productivity while others seek to learn about employee engagement.

## 3: Gig Workers

32% of organizations are replacing full -time employees with contingent workers as a cost-saving measure.

## 4: Social Safety Net

The pandemic has increased the trend of employers playing an expanded role in their employees' financial, physical and mental well-being. Support includes enhanced sick leave, financial assistance, adjusted hours of operation and child care provisions.

## 5: Skills and Roles

Before COVID-19, critical roles were viewed as roles with critical skills, or the capabilities an organization needed to meet its strategic goals.

Now, employers are realizing that they need to offer greater career development support to employees in critical roles who lack critical skills.

## 6: (De-)Humanization

Organizations are becoming more polarized in how they treat their employees. While some organizations have prioritized the well-being of employees as people, others have pushed employees to work in conditions that are high risk with little support.

## 7: Transparency

Prior to COVID-19, organizations were already facing increased employee demands for transparency. The trend has progressed to open and frequent communication to show how they are supporting employees despite the implementation of cost-saving measures.

## 8: Efficiency/Resilience

In 2019, 55% of organizational redesigns were focused on increased efficiency. This came at a cost of flexibility to respond to disruptions. The trend is now towards a more responsive organization, with employees given varied, adaptive and flexible roles so they acquire cross-functional knowledge and training.

## 9: Complexity

Post-pandemic. companies will focus on expanding their geographic diversification to mitigate and manage risk in times of disruption. This will have a negative impact on employee experience.

## What This Means

Management will need to focus on improving digital collaboration, employee experience and performance evaluation in order to improve employee retention while improving productivity.

If you'd like to comment on this article or explore these ideas further, contact me at maria@tmcconsulting.ca.



*Maria is a skilled researcher and oversees TMC benchmarking studies.*