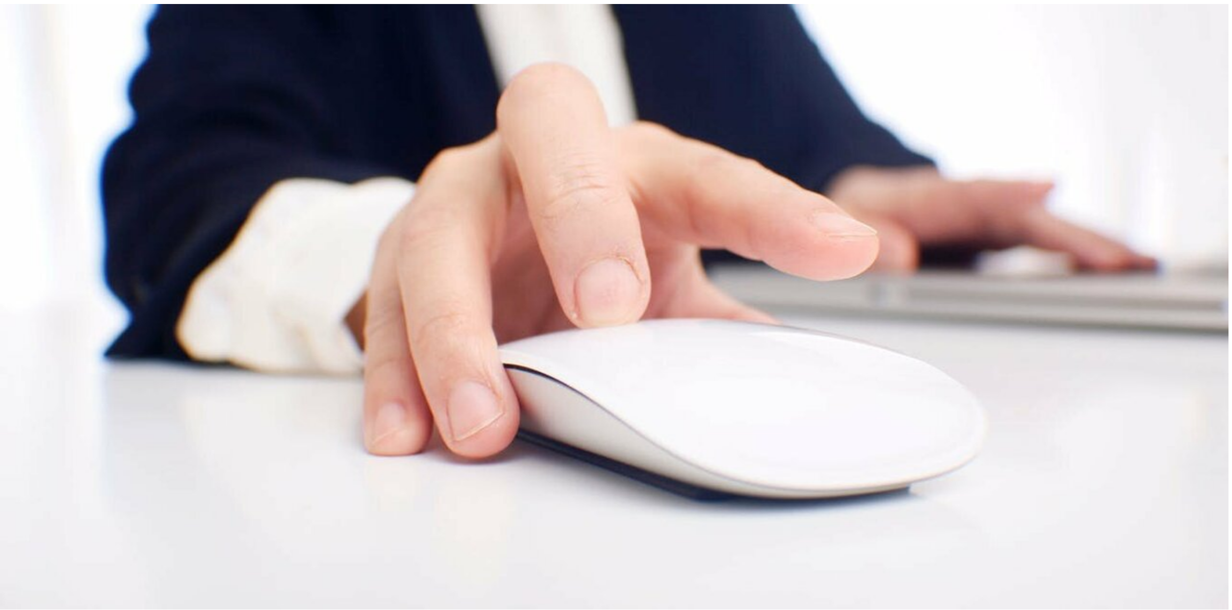
Don't click that link! How criminals access your digital devices and what happens when they do

February 11 2019, by Richard Matthews And Kieren Nicôlas Lovell



A link is a mechanism for data to be delivered to your device. Credit: Unsplash/Marvin Tolentino

Every day, often multiple times a day, you are invited to click on links sent to you by brands, politicians, friends and strangers. You download apps on your devices. Maybe you use QR codes.

Most of these activities are secure because they come from sources that can be trusted. But sometimes criminals impersonate trustworthy sources to get you to click on a link (or download an app) that contains malware.

At its core, a link is just a mechanism for data to be delivered to your device. Code can be built into a website which redirects you to another site and downloads malware to your device en route to your actual destination.

When you click on unverified links or download suspicious apps you increase the risk of exposure to malware. Here's what could happen if you do – and how you can minimise your risk.

What is malware?

Malware is defined as malicious code that: "will have adverse impact on the confidentiality, integrity, or availability of an information system."

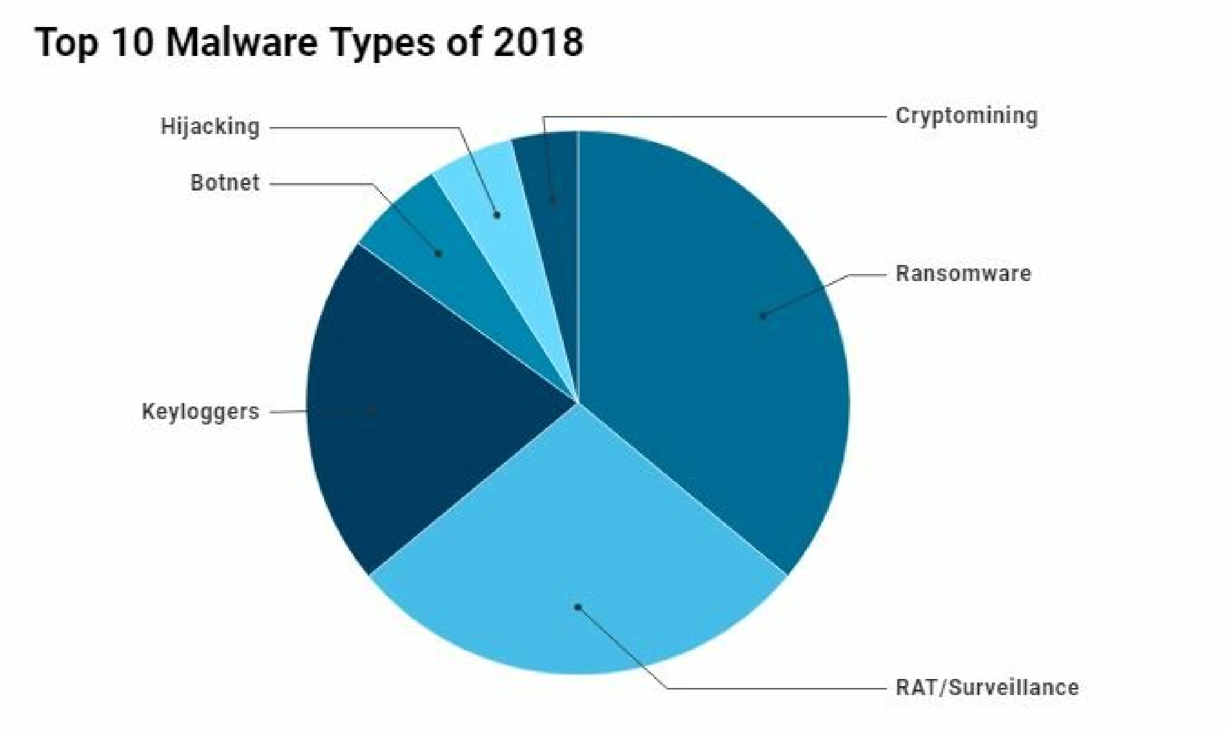
In the past, malware described malicious code that took the form of viruses, worms or Trojan horses.

Viruses embedded themselves in genuine programs and relied on these programs to propagate. Worms were generally stand alone programs that could install themselves using a network, USB or email program to infect other computers.

Trojan horses took their name from the gift to the Greeks during the Trojan war in Homer's Odyssey. Much like the wooden horse, a Trojan Horse looks like a normal file until some predetermined action causes the code to execute.

Today's generation of attacker tools are far more sophisticated, and are often a blend of these techniques.

These so-called "blended attacks" rely heavily on social engineering—the ability to manipulate someone to doing something they wouldn't normally do – and are often categorised by what they ultimately will do to your systems.



Credit: Richard Matthews

What does malware do?

Today's malware comes in easy to use, customised toolkits distributed on the dark web or by well meaning security researchers attempting to fix problems.

With a click of a button, attackers can use these toolkits to send phishing emails and spam SMS messages to eploy various types of malware. Here are some of them.

- a remote administration tool (RAT) can be used to access a computer's camera, microphone and install other types of malware
- keyloggers can be used to monitor for passwords, credit card details and email addresses
- ransomware is used to encrypt private files and then demand payment in return for the password
- botnets are used for distributed denial of service (DDoS) attacks and other illegal activities. DDoS attacks can flood a website with so much virtual traffic that it shuts down, much like a shop being filled with so many customers you are unable to move.
- crytptominers will use your computer hardware to mine cryptocurrency, which will slow your computer down
- hijacking or defacement attacks are used to deface a site or embarrass you by posting pornographic material to your social media

How does malware end up on your device?

According to insurance claim data of businesses based in the UK, over 66% of cyber incidents are caused by employee error. Although the data attributes only 3% of these attacks to social engineering, our experience suggests the majority of these attacks would have started this way.

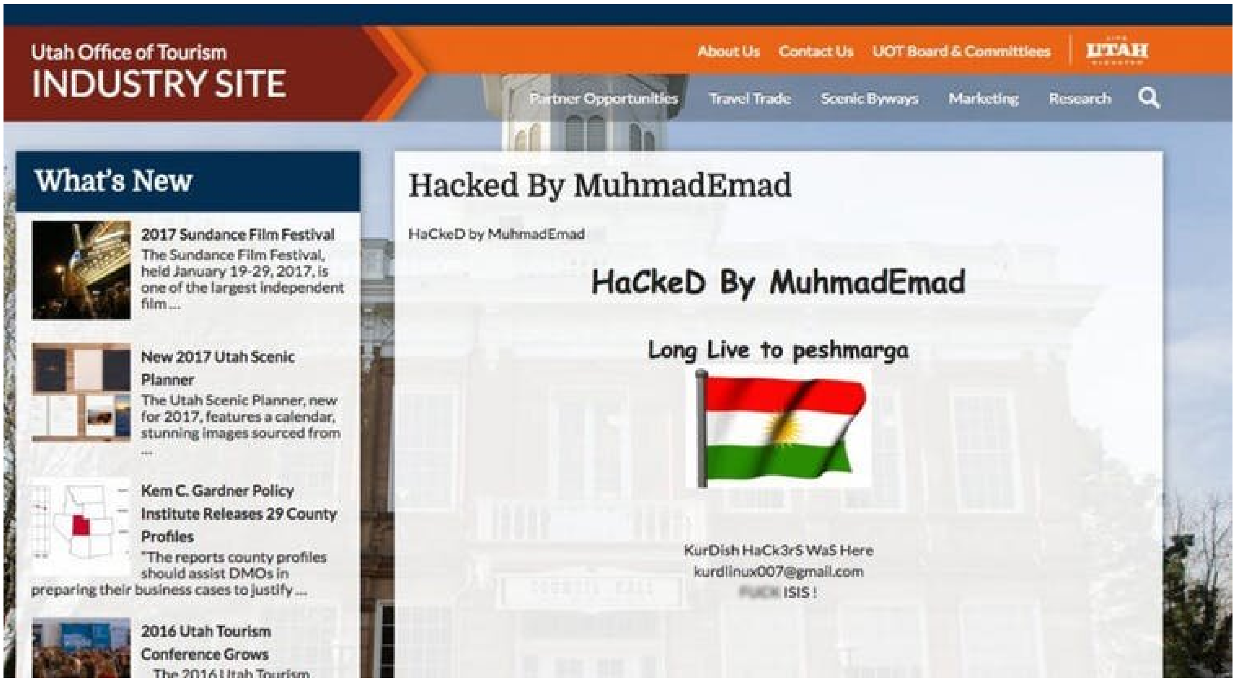
For example, by employees not following dedicated IT and information security policies, not being informed of how much of their digital footprint has been exposed online, or simply being taken advantage of. Merely posting what you are having for dinner on social media can open you up to attack from a well trained social engineer.

QR codes are equally as risky if users open the link the QR codes point to without first validating where it was heading, as indicated by this 2012 study.

Even opening an image in a web browser and running a mouse over it can lead to malware being installed. This is quite a useful delivery tool considering the advertising material you see on popular websites.

Fake apps have also been discovered on both the Apple and Google Play stores. Many of these attempt to steal login credentials by mimicking well known banking applications.

Sometimes malware is placed on your device by someone who wants to track you. In 2010, the Lower Merion School District settled two lawsuits brought against them for violating students' privacy and secretly recording using the web camera of loaned school laptops.



What's New

2017 Sundance Film Festival
The Sundance Film Festival, held January 19-29, 2017, is one of the largest independent film ...

New 2017 Utah Scenic Planner
The Utah Scenic Planner, new for 2017, features a calendar, stunning images sourced from ...

Kem C. Gardner Policy Institute Releases 29 County Profiles
"The reports county profiles should assist DMOs in preparing their business cases to justify ...

2016 Utah Tourism Conference Grows
The 2016 Utah Tourism

Hacked By MuhmadEmad

HaCkeD by MuhmadEmad

HaCkeD By MuhmadEmad

Long Live to peshmarga

KurDish HaCk3rS WaS Here
kurdlinux007@gmail.com
[redacted] ISIS !

An example of a defacement attack on The Utah Office of Tourism Industry from 2017. Credit: Wordfence

What can you do to avoid it?

In the case of the the Lower Merion School District, students and teachers suspected they were being monitored because they "saw the green light next to the webcam on their laptops turn on momentarily."

While this is a great indicator, many hacker tools will ensure webcam lights are turned off to avoid raising suspicion. On-screen cues can give you a false sense of security, especially if you don't realise that the microphone is always being accessed for verbal cues or other forms of tracking.

Basic awareness of the risks in cyberspace will go a long the way to mitigating them. This is called cyber hygiene.

Using good, up to date virus and malware scanning software is crucial. However, the most important tip is to update your device to ensure it has the latest security updates.

Hover over links in an email to see where you are really going. Avoid shortened links, such as bit.ly and QR codes, unless you can check where the link is going by using a URL expander.

What to do if you already clicked?

If you suspect you have malware on your system, there are simple steps you can take.

Open your webcam application. If you can't access the device because it is already in use this is a telltale sign that you might be infected. Higher than normal battery usage or a machine running hotter than usual are also good indicators that something isn't quite right.

Make sure you have good anti-virus and anti-malware software installed. Estonian start-ups, such as Malware Bytes and Seguru, can be installed on your phone as well as your desktop to provide real time protection. If you are running a website, make sure you have good security installed. Wordfence works well for WordPress blogs.

More importantly though, make sure you know how much data about you has already been exposed. Google yourself – including a Google image search against your profile picture – to see what is online.

Check all your email addresses on the website haveibeenpwned.com to see whether your passwords have been exposed. Then make sure you never use any passwords again on other services. Basically, treat them as compromised.

Cyber security has technical aspects, but remember: any attack that doesn't affect a person or an organisation is just a technical hitch. Cyber attacks are a human problem.

The more you know about your own digital presence, the better prepared you will be. All of our individual efforts better secure our organisations, our schools, and our family and friends.

Provided by The Conversation

Citation: Don't click that link! How criminals access your digital devices and what happens when they do (2019, February 11) retrieved 14 May 2024 from https://phys.org/news/2019-02-dont-click-link-criminals-access.html