Phishing is one of the most longstanding and dangerous methods of cyber crime. It uses deceptive messages to trick victims into clicking bogus links, downloading malicious attachments or sending sensitive information.

Despite what people think they know about phishing, they consistently fall victim. According to Verizon's 2019 Data Breach Investigations Report, 32% of all cyber attacks involved phishing.

In this presentation, I use real-life examples to demonstrate five clues to help you spot phishing scams.

SLIDE

# 1. The message is sent from a public email domain

No legitimate organisation will contact you from an address that ends '@gmail.com'.

Not even Google.

With the exception of independent workers, every organisation will have its own email domain and company accounts. For example, emails from Google will read '@google.com'.

If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate. The best way to check an organisation's domain name is to type the company's name into a search engine.

This makes detecting phishing seem easy, but cyber criminals have plenty of tricks up their sleeves to deceive you.

- ## Look at the email address, not just who the email is from

Many of us don't ever look at the email address that a message has come from. Your inbox displays a name, like 'IT Governance', and the subject line. When you open the email, you already know (or think you know) who the message is from and jump straight into the content.

When crooks create their bogus email addresses, they often have the choice to select the display name, which doesn't have to relate to the email address at all. They can therefore use a bogus email address that will turn up in your inbox with the display name Google.

But criminals rarely depend on their victim's ignorance alone. Their bogus email addresses will use the spoofed organisation's name in the local part of the address. Take this example of a scam mimicking PayPal:

SLIDE

This is a nearly flawless scam email. It uses PayPal's logo at the top of the message, it is styled professionally and the request is believable.

But as much as it attempts to replicate a genuine email from PayPal, there's one huge red flag: the sender's address is 'paypal@notice-access-273.com'.

A genuine email from PayPal would have the organisation's name in the domain name, indicating that it had come from someone at (@) PayPal. That PayPal isn't in the domain name is proof that this is a scam.

Alas, simply including PayPal anywhere in the message is often enough to trick people. They might glance at the word PayPal in the email address and be satisfied, or simply not understand the difference between the domain name and the local part of an email address.

## 2. Domain names are misspelled

There's another clue hidden in domain names that provide a strong indication of phishing scams – and it unfortunately complicates our previous clue.

The problem is that anyone can buy a domain name from a registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed.

SLIDE

For example, the domain "mycompany.com is similar to "myc0mpany.com". "greatmedia.com" is similar to "greatrnedia.com"

The hacker bought the domain “greatrnedia.com” (that’s r-n-e-d-i-a, rather than m-e-d-i-a) and impersonated an employee from a valid company that used “greatmedia.com” as their domain.

If a hacker were to send out 100 spoofed emails asking for fraudulent wire transfers to be sent, and just one of them was a successful attack, they still have a very large payday coming.

SLIDE

## 3. It’s poorly written

You can often tell if an email is a scam if it contains unusual phrases and grammatical errors.

Many people will tell you that such errors are part of a ‘filtering system’ in which cyber criminals target only the most gullible people. The theory is that, if someone ignores clues about the way the message is written, they’re less likely to pick up clues during the scammer’s endgame.

However, this really only applies to outlandish schemes like the Nigerian prince scam, which everyone is familiar with.

That, and scams like it, are manually operated: once someone takes the bait, the scammer has to reply. As such, it benefits the crooks to make sure the pool of respondents contains only those who might believe the rest of the con.

But this doesn’t apply to phishing.

- **Automated attacks**

With phishing, scammers don’t need to monitor inboxes and send tailored responses. They simply dump thousands of crafted messages on unsuspecting people.

As such, there’s no need to filter out potential respondents. Doing so would not only reduce the likelihood that an attack would be successful but also help those who didn’t fall victim to alert others to the scam.

So why are so many phishing emails poorly written? The most obvious answer is that the scammers aren’t very good at writing. Remember, many

of them are from non-English-speaking countries and from backgrounds where they will have limited access or opportunity to learn the language.

With this in mind, it becomes a lot easier to spot the difference between a typo made by a legitimate sender and a scam.

- ## Look for grammatical mistakes, not spelling mistakes

When crafting phishing messages, scammers will often use a spellchecker or translation machine, which will give them all the right words but not necessarily in the right context.

Take this example of a scam imitating Windows:

SLIDE

No individual word is spelled incorrectly, but the message is full of grammatical errors that a native speaker wouldn't make, like "We detected something unusual to use an application", and a string of missed words, such as in "a malicious user might trying to access" and "Please contact Security Communication Center".

These are consistent with the kinds of mistakes people make when learning English. Any supposedly official message that's written this way is almost certainly a scam.

That's not to say any email with a mistake in it is a scam, though. Everyone makes typos from time to time, especially when they're in a hurry.

It's therefore the recipient's responsibility to look at the context of the error and determine whether it's a clue to something more sinister. You can do this by asking:

- Is it a common sign of a typo (like hitting an adjacent key)?
- Is it a mistake a native speaker shouldn't make (grammatical incoherence, words used in the wrong context)?
- Is this email a template, which should have been crafted and copy-edited?
- Is it consistent with previous messages I've received from this person?

If you're in any doubt, you should look for examples of the other clues we list here or try to contact the sender using an alternative method (in person,

by phone, via their website, an alternative email address or through an instant message client).

SLIDE

## 4. It includes suspicious attachments or links

Phishing emails come in many forms, but the one thing they all have in common is that they contain a payload. This will either be an infected attachment that you're asked to download or a link to a bogus website that requests login and other sensitive information.

SLIDE

- ### What is an infected attachment?

An infected attachment is a seemingly benign document that contains malware. In a typical example, like this one, the phisher claims to be sending an invoice:

It doesn't matter whether the recipient expects to receive an invoice from this person or not, because in most cases they won't be sure what the message pertains to until they open the attachment.

When they open the attachment, they'll see that the invoice isn't intended for them, but it will be too late. The document unleashes malware on the victim's computer, which could perform any number of nefarious activities.

We advise that you never open an attachment unless you are fully confident that the message is from a legitimate party. Even then, you should look out for anything suspicious in the attachment.

For example, if you receive a pop-up warning about the file's legitimacy or the application asks you to adjust your settings, then don't proceed. Contact the sender through an alternative means of communication and ask them to verify that it's legitimate.

SLIDE

- ### Suspicious links

You can spot a suspicious link if the destination address doesn't match the context of the rest of the email. For example, if you receive an email from

Netflix, you would expect the link to direct you towards an address that begins ‘netflix.com’.

Unfortunately, many legitimate and scam emails hide the destination address in a button, so it’s not immediately obvious where the link goes to.

*Source: Malware Traffic Analysis*

In this example, you would probably know that something was suspicious if you saw the destination address in the email. Unfortunately, the rest of the message is pretty convincing, and you might click the link without giving it a second thought.

To ensure you don’t fall for schemes like this, you must train yourself to check where links go before opening them. Thankfully, this is straightforward: on a computer, hover your mouse over the link and the destination address appears in a small bar along the bottom of the browser.

On a mobile device, hold down on the link and a pop-up will appear containing the link.

SLIDE

## 5. The message creates a sense of urgency

Scammers know that most of us procrastinate. We receive an email giving us important news, and we decide we’ll deal with it later.

But the longer you think about something, the more likely you are to notice things that don’t seem right. Maybe you realise that the organisation doesn’t contact you by that email address, or you speak to a colleague and learn that they didn’t send you a document.

Even if you don’t get that ‘a-ha’ moment, coming back to the message with a fresh set of eyes might help reveal its true nature.

That’s why so many scams request that you act now or else it will be too late. This has been evident in every example we’ve used so far. PayPal, Windows and Netflix all provide services that are regularly used, and any problems with those accounts could cause immediate inconveniences.

SLIDE

- **The business depends on you**

The manufactured sense of urgency is equally effective in workplace scams. Criminals know that most of us will drop everything if our boss emails us with a vital request, especially when other senior colleagues are supposedly waiting on you. A typical example looks like this:

*Source: MailGuard*

Phishing scams like this are particularly dangerous because, even if the recipient did suspect foul play, they might be too afraid to confront their boss. If they were wrong, they have not only failed to meet their boss' urgent request but also implied that there was something unprofessional in the way the email was written.

An organisation that values cyber security would accept that it's better to be safe than sorry and perhaps even congratulate the employee for their caution. However, unless the organisation explicitly tells staff to remain vigilant, they might not be willing to speak up.

SLIDE

Here are some examples of actual phishing emails received at the diocese. These all relate a "sense of urgency" and can be very convincing under the right circumstances.
SLIDE
This one was sent to me. SLIDE
It conveys urgency and fear of a password no longer working, possibly my network account being locked.
SLIDE

Know what resources that are available to you. There is quite a bit of useful information on the diocesan website that can help you strengthen your security at your parishes. I recommend partnering with your IT support personnel and starting with the Quick Start guide that I have handed out to you.
This gives a good overview of best practices with examples of products available to you, data backup programs, firewalls, anti-virus, etc. the products marked with an asterisk are currently in use at the diocese and I can get you more info if you need it.

SLIDE

# Prevent phishing by helping your employees

The advice in this presentation shows how important it is for individuals to recognise signs of phishing. Spam filters will never be fully effective, so it’s up to each of us to read the context of messages and look for anything suspicious.

Organisations must therefore encourage employees to understand and analyse the way phishing works and what to do if they receive a malicious email.

If you have any further questions or would like more information, please feel free to reach out to me at the diocese.