Exmo/a Senhor/a Encarregado/a de Educação,

Vivemos numa época sem precedentes. Ainda há pouco tempo a Covid-19 era considerada para a maioria das pessoas uma doença anónima e distante, que infetava pessoas "do outro lado do mundo". Hoje, está no centro das nossas vidas, altera relações e comportamentos, condiciona o nosso quotidiano e tem implicações que dificilmente conseguimos antever.

A atual mudança de paradigma com a saída do habitual local de trabalho e a permanência nas nossas residências pode colocar-nos em risco em situações que, normalmente, não estaríamos à espera. Além disso, o ritmo e as distrações domésticas, a vertigem desinformativa das redes sociais e a incerteza, aumentam a nossa vulnerabilidade. Este cenário pode ser explorado pelos que vivem do crime e da fraude informática (são várias as ameaças, com destaque para o phishing e o pharming).

Phishing ou pharming.

Tentativas de obtenção de informações sensíveis assumindo de forma fraudulenta a identidade de uma fonte legítima. O **phishing** tem por base o e-mail, enquanto o **pharming** utiliza websites e servidores falsos. Estar informado é vital para ajudar os colaboradores a evitar esta tática.

Procurando dar continuidade a uma postura pedagogicamente serena mas ativa, e renovando o nosso compromisso no acompanhamento à comunidade escolar, vimos por este meio partilhar as seguintes recomendações:

- Mantenha a calma e a serenidade;
- Tenha como referência informação rigorosa, obtida em fontes credíveis e bem identificadas (afaste-se de fontes pouco fidedignas ou desconhecidas). Desconfie de mensagens alarmistas, de fontes desconhecidas, e que solicitem ações de "urgência";
- Não seja foco de difusão de notícias catastrofistas, e de origens desconhecidas: é frequente estas mensagens estarem infetadas com malware informático, sendo por isso focos de disseminação de vírus, causando danos de vários tipos;
- Adote uma especial atenção à origem de mensagens de email ou de redes sociais, incluindo WhatsApp, e à fidedignidade da sua origem;
- Adote uma especial precaução em relação a links encurtados;

- Em nenhuma situação entregue as suas credenciais (username e passwords), ou as mude, por solicitação de mensagem recebida por email ou nas redes sociais;
- Não abra anexos de mensagens não solicitadas, mesmo que pareçam enviadas por conhecidos (o computador ou a conta de um amigo que estejam comprometidos podem enviar e-mails malignos; desconfie se parecer que a mensagem foi enviada para toda a lista de endereços dessa pessoa);
- Desconfie de mensagens com endereços estranhos ou com português incorreto;
- Se por alguma razão, desconfiar que foi vítima de phishing, ou de outro tipo de ataque similar, reporte-o de imediato às autoridades competentes;

Uma vez mais, obrigado por toda a vossa confiança.

Atentamente,
A Direção do Colégio Valsassina
18.03.2020